VB104W VDSL

User Manual

Contents

1 Safety Precautions 1
2 Overview 2
2.1 Packing List 2
2.2 Application 2
2.3 Features 3
2.4 Standards Compatibility and Compliance 4
3 Hardware Description and Installation 5
3.1 LEDs and Interfaces 5
3.2 Hardware Installation 7
4 PC Network Configuration and Login 9
4.1 PC Network Configuration 9
4.2 Logging in to the DSL Router 10
5 Web-based Management 11
5.1 Setup 11
5.1.1 Wizard 11
5.1.2 Internet Setup 20
5.1.3 Wireless 23
5.1.4 Local Network 28
5.1.5 Local IPv6 Network 31
5.1.6 Time and Date 33
5.2 Advanced 34
5.2.2 ALG 40
5.2.3 Port Forwarding 41
5.2.4 DMZ 43
5.2.5 Parental Control 44
5.2.6 Filtering Options 48
5.2.7 QoS Configuration 53
5.2.8 Anti-Attack Settings 59
5.2.9 DNS 60
5.2.10 Dynamic DNS 61
5.2.11 Network Tools 62
5.2.12 Routing 72
5.2.13 NAT 78
5.3 Management 78

5.3.1 System Management 79
5.3.2 Firmware Update 81
5.3.3 Access Controls 82
5.3.4 Diagnosis 87
5.3.5 Log Configuration 91
5.4 Status 92
5.4.1 Device Info 92
5.4.2 Wireless Clients 93
5.4.3 DHCP Clients 94
5.4.4 Logs 94
5.4.5 Statistics 95
5.4.6 Route Info 96
5.5 Help 97
6 Trouble Shooting 98

1 Safety Precautions

Take the following instructions to prevent the device from risks and damage caused by fire or electric power.

- Use the type of power marked in the volume label.
- Use the power adapter in the product package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines or plugs may cause electric shock or fire accidents. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a heat source or under a high temperature occurs. Keep the device away from direct sunshine.
- Do not put this device close to an overdamp or watery place. Do not spill fluid on this device.
- Do not connect this device to a PC or electronic product unless instructed by our customer engineer or your broadband provider. Wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

2 Overview

The VB104W VDSL Router integrates wireless LAN and USB service into one unit. It is designed to provide a simple and cost-effective DSL Internet connection for a private Ethernet and 802.11g/802.11b/802.11n wireless network. The Router combines high-speed DSL Internet connection, IP routing for the LAN, and wireless connectivity in one package.

The Router is easy to install and use. The Router connects to an Ethernet LAN or computers via standard Ethernet ports. The DSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet by a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

Network and Router management is done through the web-based management interface accessed through the local Ethernet using any web browser. You may also enable remote management to enable configuration of the Router via the WAN interface.

2.1 Packing List

2.2 Application

- Home gateway
- Wireless LAN
- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- Audio and video streaming and transfer
- Network and online gaming

2.3 Features

- User-friendly GUI for web configuration
- Compatible with all standard Internet applications
- Industry standard and interoperable xDSL interface
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 8 permanent virtual circuits (PVC)
- Support for up to 8 PPPoE sessions
- Support RIP v1 & RIP v2
- WLAN with high-speed data transfer rates, compatible with IEEE 802.11b/g/n
- IP routing and bridging
- Asynchronous transfer mode (ATM) , PTM (Packet Transfer mode), and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)
- Web filtering
- Management and control

  Web-based management (WBM)

  Command line interface (CLI)

  TR-069 WAN management protocol
- Remote update
- System statistics and monitoring
- DSL router is targeted at the following platforms: DSL modems, wireless access points and bridge.
- Multicast listener discovery (MLD)
- Internet group management protocol (IGMP)
- Application layer gateway (ALG)

2.4 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ITU G.993.1 (VDSL)
- ITU G993.2 (VDSL2)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

3 Hardware Description and Installation

3.1 LEDs and Interfaces

Front Panel

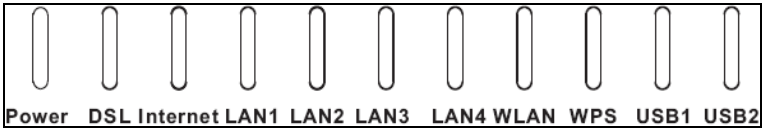


Figure 1 Front panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	The device is powered on.
		Off	The device is powered off.
	Red	On	Self-test fails, or failure occurs, or the device is starting.
DSL	Green	On	DSL link is established.
		Slow Blink	The DSL line is attempting to detect signals.
		Fast Blink	Signals have been detected, and the DSL line is attempting to establish link.
Internet	Green	On	Physical layer connection and IP connection is established in routing mode.
		Blink	IP connection is established, and messages are being transmitted.
		Off	IP connection or physical layer link is not established.
	Red	On	IP connection fails.
LAN 1/2/3/4	Green	On	Ethernet link is established.
		Blink	Data is being transmitted through a LAN interface.
		Off	Ethernet link is not established.
WLAN	Green	On	WLAN is enabled.

Indicator	Color	Status	Description
		Blink	Data is being transmitted by the wireless module.
		Off	WLAN is disabled.
WPS	Green	On	Negotiation is successful under Wi-Fi protected setup.
		Blink	Negotiation is in progress under Wi-Fi protected Setup.
		Off	Wi-Fi protected setup is disabled.
USB	Green	On	A USB device is connected.
		Blink	Data is being transmitted.
		Off	No USB connection.

Rear Panel

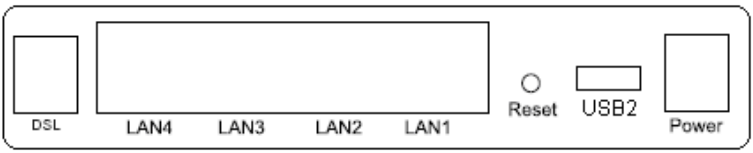


Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
DSL	RJ-11 interface connecting to a telephone set through a telephone cable
LAN1/2/3/4	Ethernet RJ-45 interfaces connecting to the Ethernet interfaces of computers or Ethernet devices
Reset	Reset to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button for more than 5 seconds and then release.
USB2	USB port, for connecting USB devices.

Interface/Button	Description
Power	Interface connecting to the power adapter. The power adapter output is: 12V DC, 1000mA

Side Panel

Interface/Button	Description
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button, and then the wireless router starts to accept the negotiation of PBC mode.
WLAN	WLAN switch, for enabling or disabling the WLAN function.
USB1	USB port, for connecting USB devices.
ON/OFF	Push to power on/off the device.

3.2 Hardware Installation

Step 1 Connect the **DSL** port of the device and the **Modem** port of the splitter with a telephone cable. Connect the phone to the **Phone** port of the splitter through a telephone cable. Connect the incoming line to the **Line** port of the splitter.

The splitter has three ports:

- Line: Connect to a wall phone port (RJ-11 jack).
- Modem: Connect to the DSL port of the device.
- Phone: Connect to a telephone set.

Step 2 Connect a **LAN** port of the device to the network card of the PC through an Ethernet cable (MDI/MDIX).

Note:

Use twisted-pair cables to connect the device to a Hub or switch.

Step 3 Plug one end of the power adapter to the wall outlet and the other end to the **Power** port of the device.

Connection: Figure 3 displays the application diagram for the connection of the device, PC, splitter and telephone sets, when no telephone set is placed before the splitter.

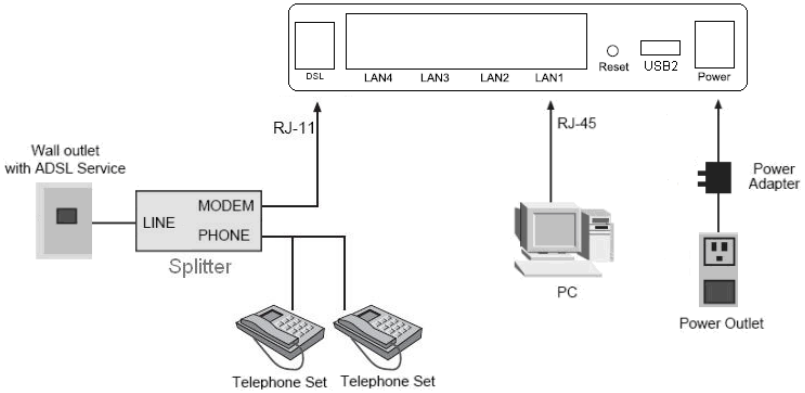


Figure 3 Connection diagram (without telephone sets before the splitter)

Installing a telephone directly before the splitter may lead to failure of connection between the device and the central office, or failure of Internet access, or slow connection speed. If you really need to add a telephone set before the splitter, you must add a microfilter before a telephone set. Do not connect several telephones before the splitter or connect several telephones with the microfilter.

4 PC Network Configuration and Login

4.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

The following displays the **TCP/IP Properties** dialog box on Windows XP.

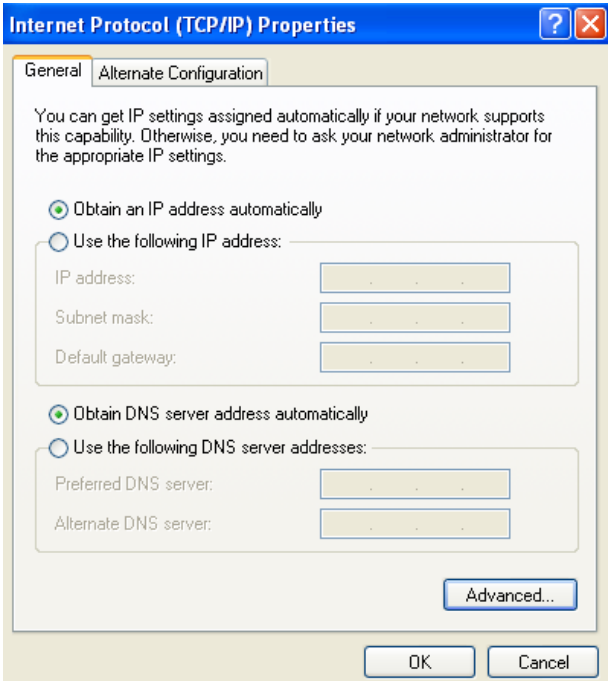

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 4 PC Network Configuration

TCP/IP configuration steps for Windows XP are as follows:

Step 1 Choose Start > Control Panel > Network Connections.

Right-click the Ethernet connection icon and choose **Properties**.

On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**. The Internet Protocol (TCP/IP) Properties window appears.

Select the **Obtain an IP address automatically** radio button.

Select the **Obtain DNS server address automatically** radio button.

Click **OK** to save the settings.

4.2 Logging in to the DSL Router

To log in to the DSL router, do as follows.

Step 1 Open a Web browser on your computer.

Step 2 Enter ***http://192.168.1.1*** (default IP address of the DSL router) in the address bar. The login page appears.

Step 3 Enter the user name and the password. The default username and password are **admin** and **admin**. The username and password of the common user are **user** and **user**. The username and password of the support account are **support** and **support**.

Step 4 You need not enter the username and the password again if you select the browser option **Remember my password**. It is recommended to change these default values after logging in to the DSL router for the first time.

Step 5 Click **OK** to log in to the Web page. Otherwise, please click **Cancel** to exit the login page.

After logging in to the DSL router as a super user, you can query, configure, and modify all the settings, and diagnose the system.

5 Web-based Management

This chapter describes how to use Web-based management of the DSL router, which allows you to configure and control all of DSL router features and system parameters in a user-friendly GUI.

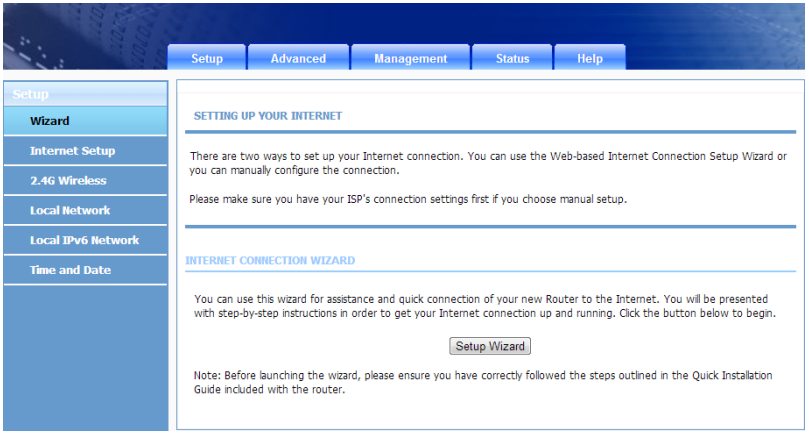
5.1 Setup

In the main interface, click **Setup** tab to enter the **Setup** menu as shown in the following figure. The submenus are **Wizard**, **Internet Setup**, **Wireless**, **Local Network**, **Local IPv6 Network**, **Time and Date** and **Logout**.

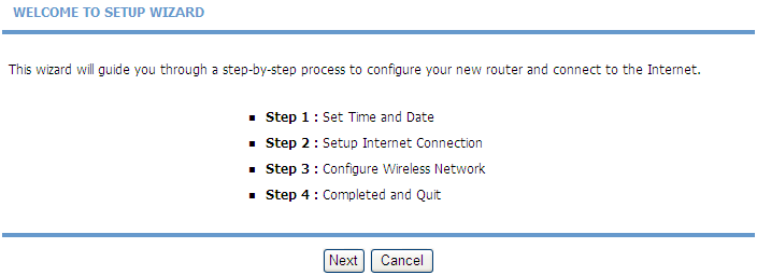
5.1.1 Wizard

Wizard enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe configuration parameters. When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. Your physical WAN device can be Ethernet, DSL or both. Technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you that you are connected to the Internet using a static or dynamic IP address, or the protocol used for communication over the Internet, such as PPPoA or PPPoE,.

Step 1 Choose **Setup** > **Wizard**. The page shown in the following figure appears.

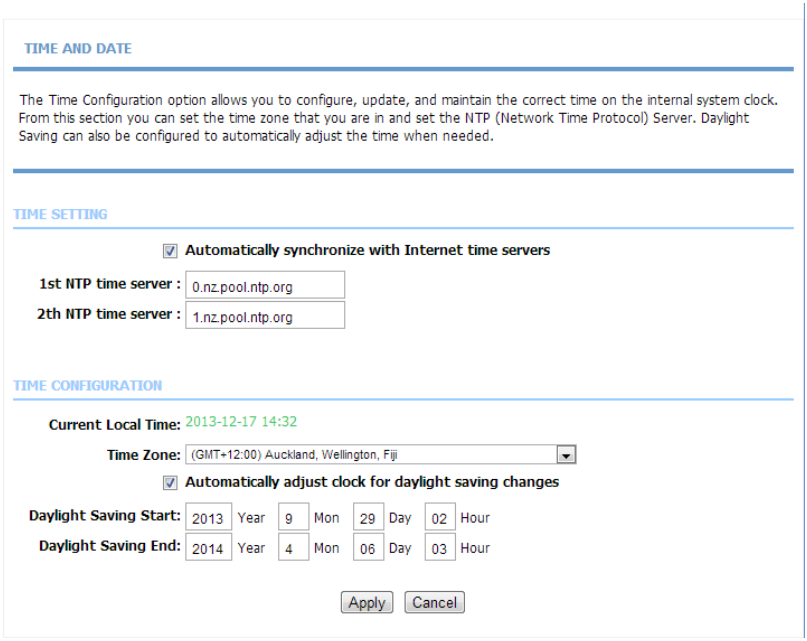

Setup
Advanced
Management
Status
Help
Setup
Wizard
Internet Setup
2.4G Wireless
Local Network
Local IPv6 Network
Time and Date
SETTING UP YOUR INTERNET
There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection.
Please make sure you have your ISP's connection settings first if you choose manual setup.
INTERNET CONNECTION WIZARD
You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.
Setup Wizard
Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

Step 2 Click **Setup Wizard**. The page shown in the following figure appears.


WELCOME TO SETUP WIZARD
This wizard will guide you through a step-by-step process to configure your new router and connect to the Internet.
Step 1 : Set Time and Date
Step 2 : Setup Internet Connection
Step 3 : Configure Wireless Network
Step 4 : Completed and Quit
Next
Cancel

Step 3 There are four steps to configure the device. Click **Next** to continue.

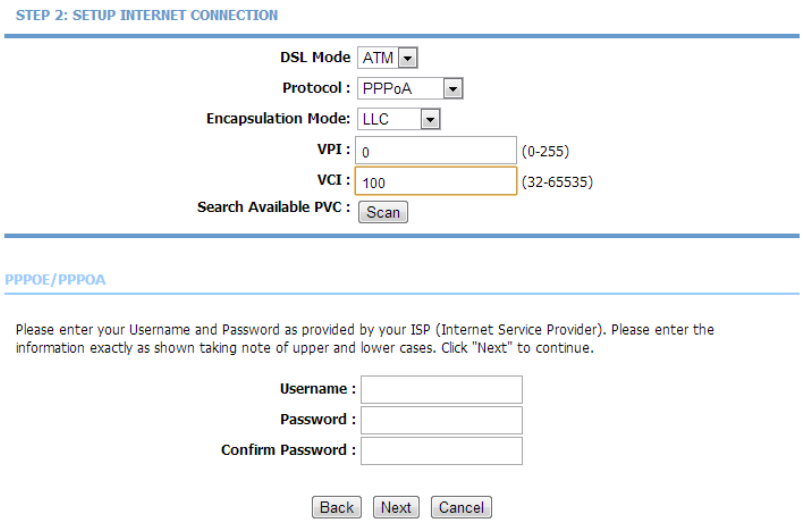
Step 4 Set the time and date.


TIME AND DATE
The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.
TIME SETTING
Automatically synchronize with Internet time servers
1st NTP time server : 0.nz.pool.ntp.org
2th NTP time server : 1.nz.pool.ntp.org
TIME CONFIGURATION
Current Local Time: 2013-12-17 14:32
Time Zone: (GMT+12:00) Auckland, Wellington, Fiji
Automatically adjust clock for daylight saving changes
Daylight Saving Start: 2013 Year 9 Mon 29 Day 02 Hour
Daylight Saving End: 2014 Year 4 Mon 06 Day 03 Hour
Apply
Cancel

Step 5 Configure the Internet connection. Set the VPI and VCI.

PPPoE/ PPPoA

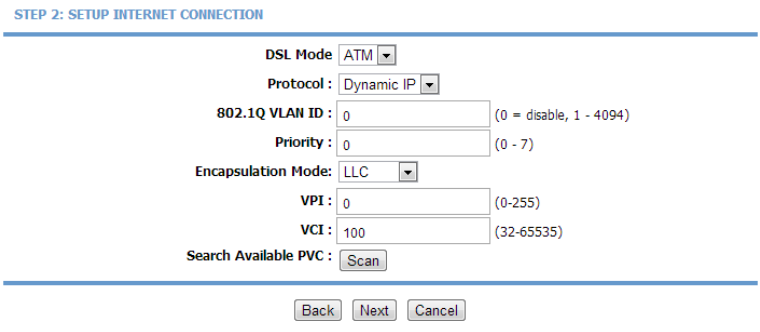
When you choose the **DSL Mode** as **ATM** and the **Protocol** as **PPPoE** or **PPPoA**, the page shown in the two following figure appears.


STEP 2: SETUP INTERNET CONNECTION
DSL Mode ATM
Protocol : PPPoA
Encapsulation Mode: LLC
VPI : 0 (0-255)
VCI : 100 (32-65535)
Search Available PVC : Scan
PPPOE/PPPOA
Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.
Username :
Password :
Confirm Password :
Back Next Cancel

In this page, enter the user name and password as provided by your ISP.

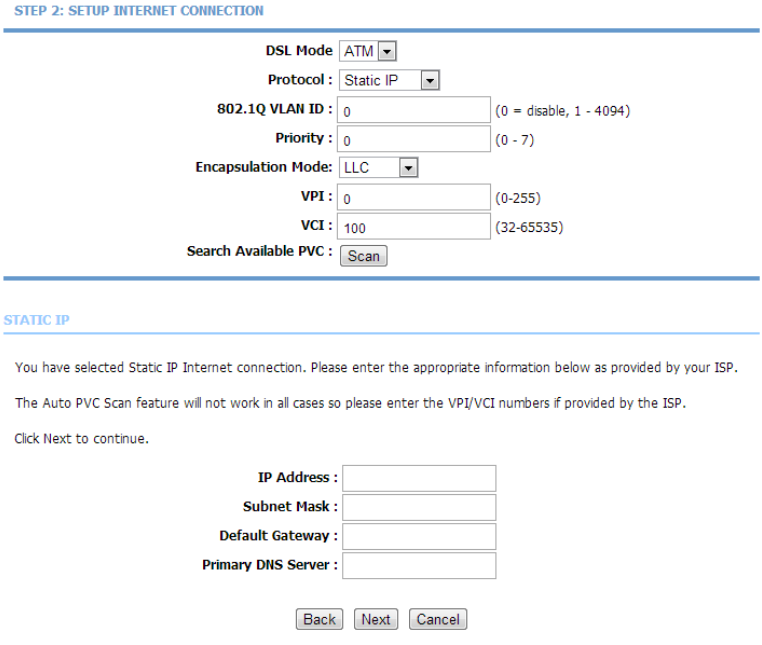
Dynamic IP

When you choose the **DSL Mode** as **ATM** and the **Protocol** as **Dynamic IP**, the page shown in the following figure appears.



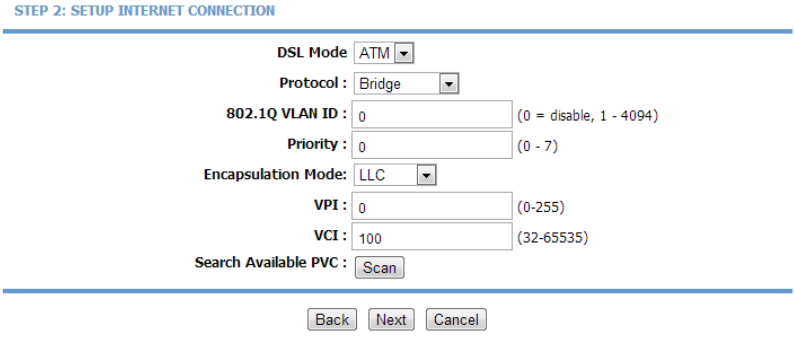
Static IP

When you choose the **DSL Mode** as **ATM** and the **Protocol** as **Static IP**, the page shown in the following figure appears. Enter the **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary DNS Server**.


STEP 2: SETUP INTERNET CONNECTION
DSL Mode ATM
Protocol : Static IP
802.1Q VLAN ID : 0 (0 = disable, 1 - 4094)
Priority : 0 (0 - 7)
Encapsulation Mode: LLC
VPI : 0 (0-255)
VCI : 100 (32-65535)
Search Available PVC : Scan
STATIC IP
You have selected Static IP Internet connection. Please enter the appropriate information below as provided by your ISP.
The Auto PVC Scan feature will not work in all cases so please enter the VPI/VCI numbers if provided by the ISP.
Click Next to continue.
IP Address :
Subnet Mask :
Default Gateway :
Primary DNS Server :
Back Next Cancel

Bridge

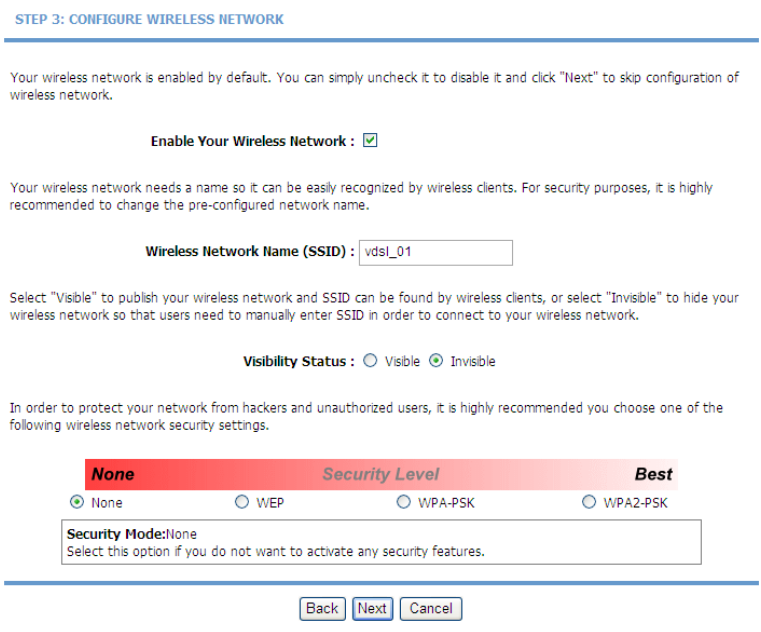
When you choose the **DSL Mode** as **ATM** and the **Protocol** as **Bridge**, the page shown in the following figure appears.


STEP 2: SETUP INTERNET CONNECTION
DSL Mode ATM
Protocol : Bridge
802.1Q VLAN ID : 0 (0 = disable, 1 - 4094)
Priority : 0 (0 - 7)
Encapsulation Mode: LLC
VPI : 0 (0-255)
VCI : 100 (32-65535)
Search Available PVC : Scan
Back Next Cancel

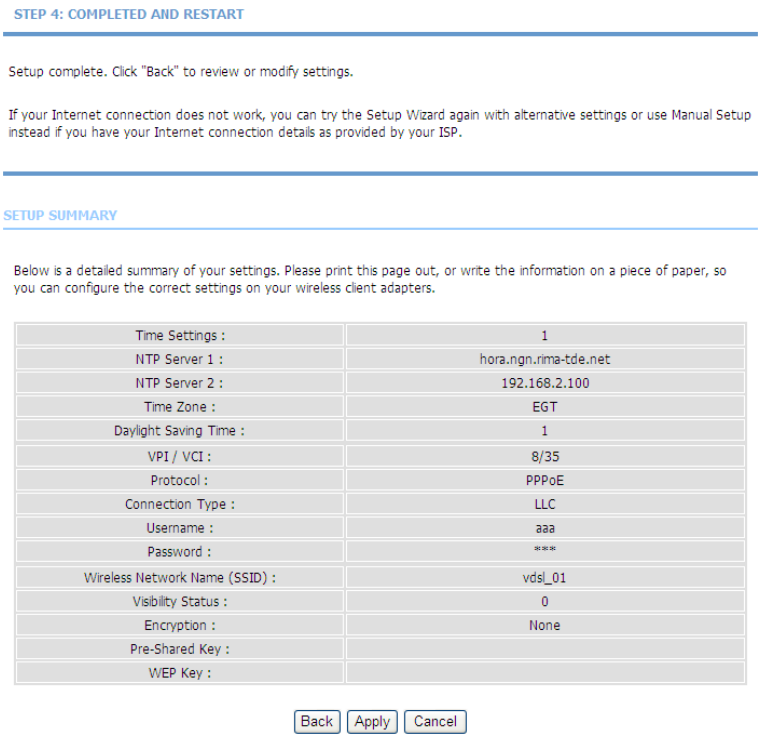
Note:

When you choose the **DSL Mode** as **PTM**, please refer to the configurations under **ATM** mode for corresponding Internet configurations.

Step 6 Click Next. The page shown in the following figure appears.


STEP 3: CONFIGURE WIRELESS NETWORK
Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.
Enable Your Wireless Network :
Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.
Wireless Network Name (SSID) : vdsl_01
Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.
Visibility Status : Visible Invisible
In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.
None
Security Level
Best
None
WEP
WPA-PSK
WPA2-PSK
Security Mode:None
Select this option if you do not want to activate any security features.
Back
Next
Cancel

Step 7 Configure the wireless network. Enter the information and click **Next**.


STEP 4: COMPLETED AND RESTART
Setup complete. Click "Back" to review or modify settings.
If your Internet connection does not work, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.
SETUP SUMMARY
Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.
Time Settings : 1
NTP Server 1 : hora.ngn.rima-tde.net
NTP Server 2 : 192.168.2.100
Time Zone : EGT
Daylight Saving Time : 1
VPI / VCI : 8/35
Protocol : PPPoE
Connection Type : LLC
Username : aaa
Password : ***
Wireless Network Name (SSID) : vdsl_01
Visibility Status : 0
Encryption : None
Pre-Shared Key :
WEP Key :
Back
Apply
Cancel

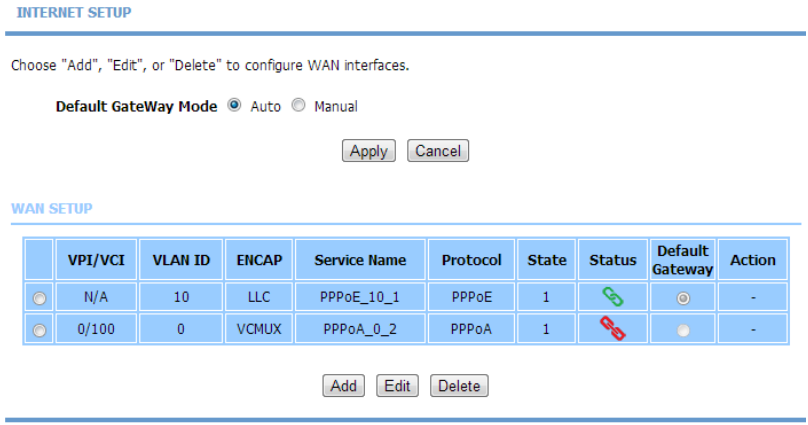
Step 8 Click **Apply** to save the settings.

Note:

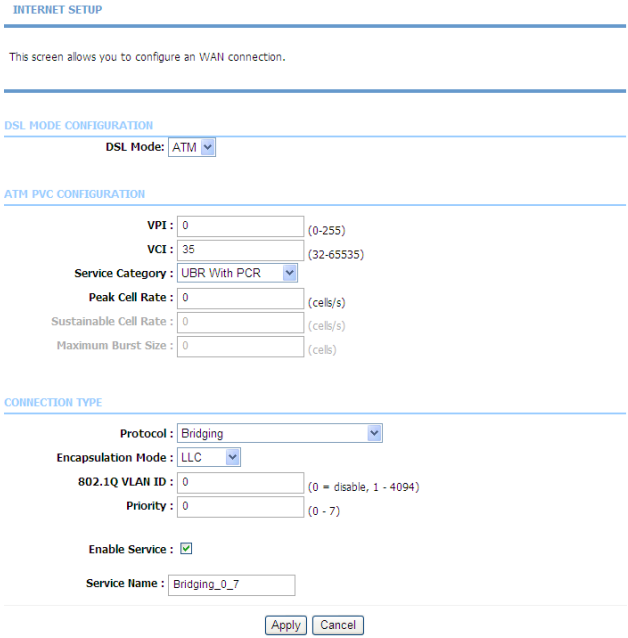
In each step of the Wizard page, you can click **Back** to review or modify the previous settings. Click **Cancel** to exit the wizard page.

5.1.2 Internet Setup

Choose **Setup** > **Internet Setup**. The page shown in the following figure appears. In this page, you can configure the WAN interface of the device.



Click **Add** in **"INTERNET SETUP"**. The page shown in the following figure appears.

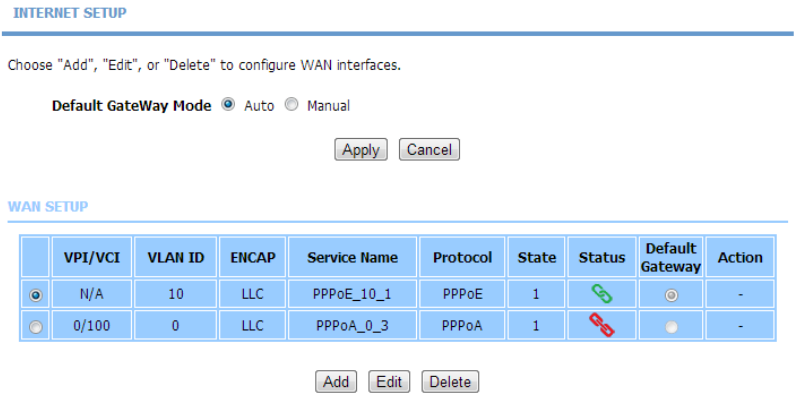

INTERNET SETUP
This screen allows you to configure an WAN connection.
DSL MODE CONFIGURATION
DSL Mode: ATM
ATM PVC CONFIGURATION
VPI : 0 (0-255)
VCI : 35 (32-65535)
Service Category : UBR With PCR
Peak Cell Rate : 0 (cells/s)
Sustainable Cell Rate : 0 (cells/s)
Maximum Burst Size : 0 (cells)
CONNECTION TYPE
Protocol : Bridging
Encapsulation Mode : LLC
802.1Q VLAN ID : 0 (0 = disable, 1 - 4094)
Priority : 0 (0 - 7)
Enable Service :
Service Name : Bridging_0_7
Apply
Cancel

The following table describes the parameters in this page.

Field	Description
DSL Mode	You can select **ATM** or **PTM**.
PVC Settings	**VPI**: The virtual path between two points in an ATM network, and its valid value is from **0** to **255**. **VCI**: The virtual channel between two points in an ATM network, ranging from **32** to **65535** (0 to 31 is reserved for local management of ATM traffic).
Service Category	You can select from the drop-down list.

Field	Description
	UBR With PCR UBR Without PCR UBR With PCR CBR Non Realtime VBR Realtime VBR
Protocol	You can select from the drop-down list. Bridging PPP over ATM (PPPoA) PPP over Ethernet (PPPoE) MAC Encapsulation Routing (MER) IP over ATM (IPoA) Bridging
Encapsulation Mode	Select the method of encapsulation provided by your ISP. You can select **LLC** or **VCMUX**.

Click **Apply**, the page shown in the following figure appears.

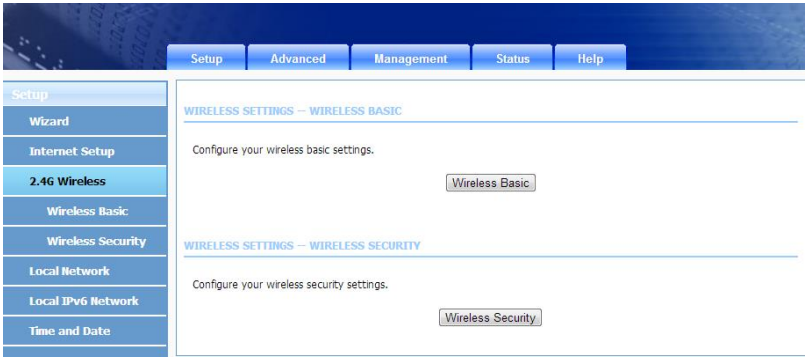


To manage the existing WAN connections, select a connection from the list, and then click **Edit** or **Delete**.

5.1.3 Wireless

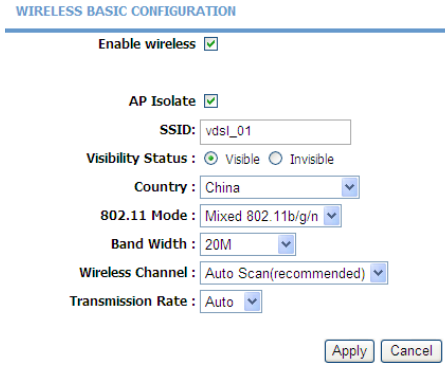
This section describes the wireless LAN and basic configuration. A wireless LAN can be as simple as two computers with wireless LAN cards communicating in a pear-to-pear network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to wired LAN.

Choose **Setup** > **Wireless**. The **Wireless** page shown in the following figure appears.



5.1.3.1 Wireless Basic

In the **Wireless** page, click **Wireless Basic**. The page shown in the following figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device.



The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select this to turn Wi-Fi on.
AP Isolate	Select this to turn AP isolation on.
Wireless Network Name (SSID)	The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.
Visibility Status	You can select **Visible** or **Invisible**.
Country	Select the country from the drop-down list.
802.11 Mode	Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are **802.11b only**, **802.11g only**, **802.11n only**, **Mixed 802.11b/g**, **Mixed 802.11n/g** and **Mixed 802.11b/g/n**.
Band Width	Select the appropriate band as **20M**, **40M Plus**, or **40M Minus** from the pull-down menu.
Wireless Channel	Select the wireless channel from the pull-down menu. It is different for different country.
Transmission	Select the transmission rate for the network. The rate

Field	Description
Rate	of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default is **Auto**.

Click **Apply** to save the settings.

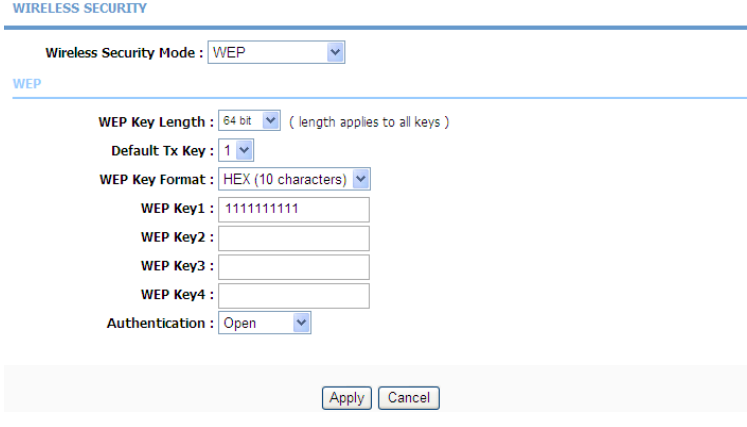
5.1.3.2 Wireless Security

In the **Wireless** page, click **Wireless Security**. The page shown in the following figure appears. Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and wired network.

Note:

Enable Wireless before configuring the wireless security settings in this page. Refer to 5.1.3.1 Wireless Basic.

When the Security Mode is set as **WEP**, the following figure appears.

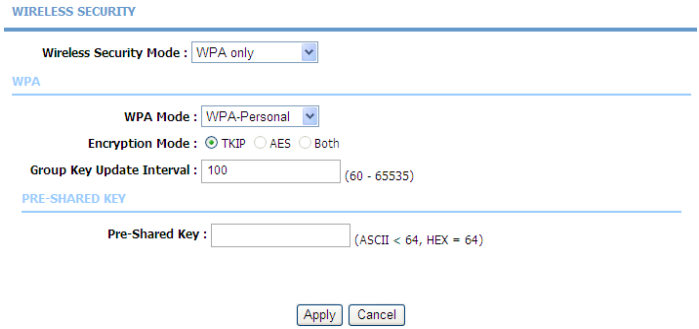


The following table describes the parameters of this page.

Field	Description
WEP Key Length	Choose the WEP key length. You can choose **64-bit** or **128-bit**.
Default Tx Key	Choose the index of WEP Key. You can choose **Key 1**, **2**, **3** or **4**.
WEP Key Format	● When **64-bit** key length is selected, you can choose **ASCII (5 characters)** or **HEX (10 characters)**. ● When **128-bit** key length is selected, you can choose **ASCII (13 characters)** or **HEX (26 characters)**.
WEP Key 1/2/3/4	The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission. The default key 1 is **1111111111**.
Authentication	Choose an authentication mode.

Click **Apply** to save the settings.

When the Security Mode is set as **WPA only**, **WPA2 only** or **WPA/WPA2 Mixed**, the following figure appears.


WIRELESS SECURITY
Wireless Security Mode : WPA only
WPA
WPA Mode : WPA-Personal
Encryption Mode : TKIP AES Both
Group Key Update Interval : 100 (60 - 65535)
PRE-SHARED KEY
Pre-Shared Key : (ASCII < 64, HEX = 64)
Apply Cancel

The following table describes the parameters in this page.

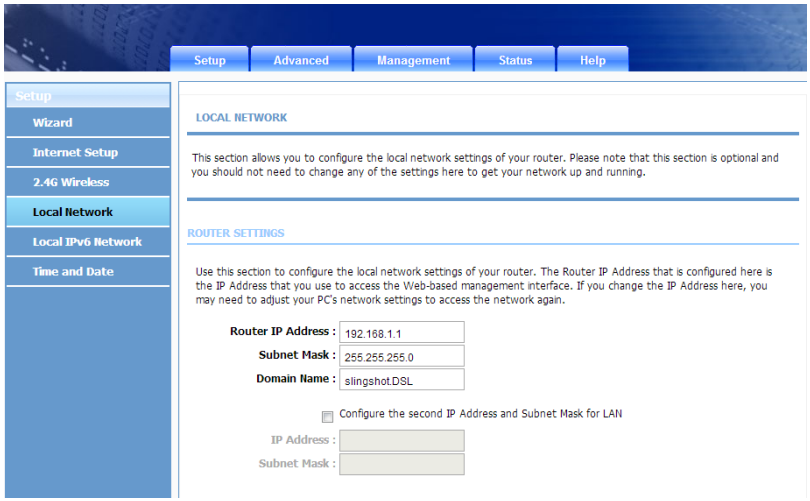
Field	Description
Wireless Security Mode	Configure the wireless encryption mode. You can choose **None**, **WEP**, **WPA Only**, **WPA2 Only** or **WPA /WPA2 Mixed**. ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA/WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA Mode	● Select **Personal**, and then enter the pre-shared key in the **Pre-Shared Key** field. ● Select **Enterprise**, and then enter the port, IP address, and password of the Radius server. You need to enter the password provided by the Radius server when the wireless client connects the modem. If the encryption is set to **WEP**, the modem uses 802.1 X authentication, which is Radius authentication.
Encryption Mode	When **WPA /WPA2 Mixed** is selected, you can select WPA encryption as **AES**, **TKIP** or **Both**.
Group Key Update Interval	When WPA encryption is applied, messages sent are encrypted with a password. For higher security, WPA password is updated periodically. This value is the update interval of the WPA password.

5.1.4 Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.1.1. You can use the default settings and DHCP service to manage the IP settings for the private network. The IP address of the device is the base address used for DHCP. To use the device for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the device. The IP address available in the DHCP IP address pool changes automatically if you change the IP address of the device.

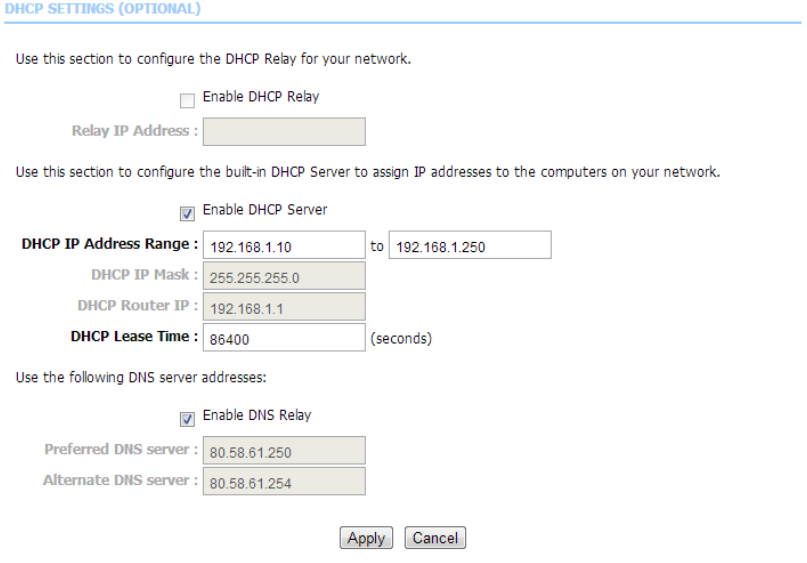
You can also enable the secondary LAN IP address. The two LAN IP addresses must be in different networks.

Choose **Setup** > **Local Network**. The **Local Network** page shown in the following figure appears.


Setup
Advanced
Management
Status
Help
Setup
Wizard
Internet Setup
2.4G Wireless
Local Network
Local IPv6 Network
Time and Date
LOCAL NETWORK
This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.
ROUTER SETTINGS
Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.
Router IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
Domain Name : slingshot.DSL
Configure the second IP Address and Subnet Mask for LAN
IP Address :
Subnet Mask :

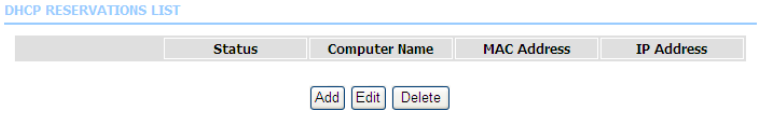
By default, **Enable DHCP Server** is selected for the Ethernet LAN interface of the device. DHCP service supplies IP settings to workstations configured to automatically obtain IP settings from a PC connected to the device through the Ethernet port. When the device is used for DHCP, it becomes the default gateway for DHCP clients connected to it. If you change the IP address of the device, you must also change the range of IP addresses in the pool used for DHCP on the LAN. The IP address pool can contain up to 253 IP addresses.

This page is used to configure the DHCP Server and DHCP Relay Settings. The **DHCP Lease Time** is at least **600** seconds and without upper limit; **-1** means unrestricted lease time.

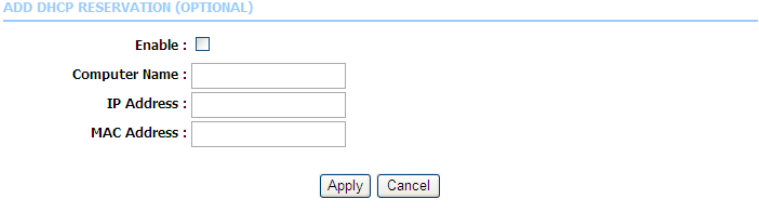

DHCP SETTINGS (OPTIONAL)
Use this section to configure the DHCP Relay for your network.
Enable DHCP Relay
Relay IP Address :
Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.
Enable DHCP Server
DHCP IP Address Range : 192.168.1.10 to 192.168.1.250
DHCP IP Mask : 255.255.255.0
DHCP Router IP : 192.168.1.1
DHCP Lease Time : 86400 (seconds)
Use the following DNS server addresses:
Enable DNS Relay
Preferred DNS server : 80.58.61.250
Alternate DNS server : 80.58.61.254
Apply
Cancel

Click **Apply** to save the settings.

In the **Local Network** page, you can assign IP addresses on the LAN to specific individual computers based on their MAC addresses.



Click **Add** to add static DHCP (optional). The page shown in the following figure appears.



Select **Enable** to reserve the IP address for the designated PC with the configured MAC address. The **Computer Name** helps you to recognize the PC with the MAC address, for example, Father's Laptop. Click **Apply** to save the settings.

After the DHCP reservation is saved, the DHCP reservations list displays the configuration.

The **NUMBER OF DYNAMIC DHCP CLIENTS** page shows the current DHCP clients (PC or Laptop) connected to the device and the detailed information of the connected computer(s).

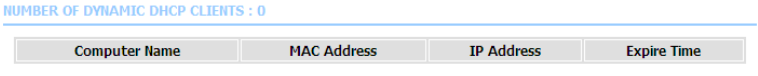
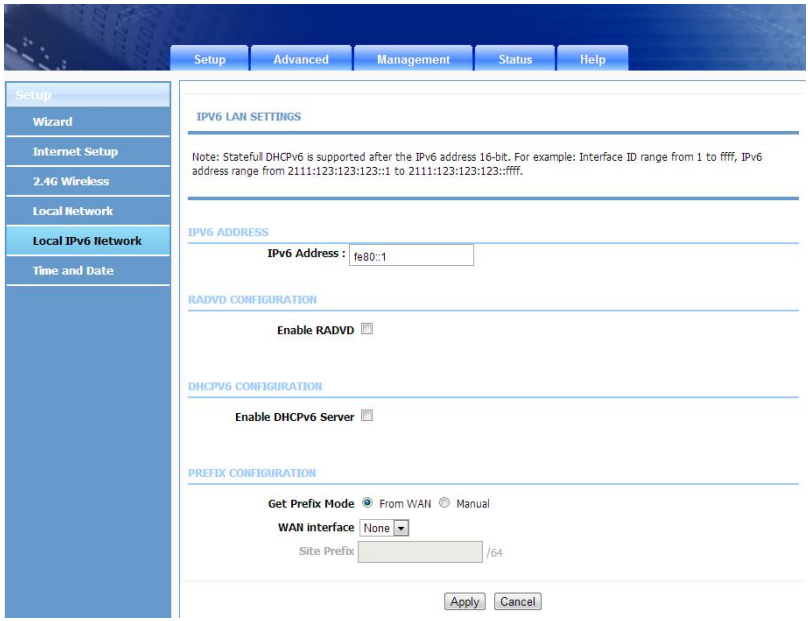


Figure 5

5.1.5 Local IPv6 Network

You can configure the LAN IPv6 address according to the actual application. The preset IPv6 address is fe80::1. You can use the default settings and DHCPv6 service to manage the IPv6 settings for the private network. The IPv6 address of the device is the base address used for DHCPv6. To use the device for DHCPv6 on your LAN, the IPv6 address pool used for DHCPv6 must be compatible with the IPv6 address of the device. The IPv6 address available in the DHCP IPv6 address pool changes automatically if you change the IPv6 address of the device.

Choose **Setup** > **Local IPv6 Network**. The page shown in the following figure appears. In this page, you can configure a static LAN IPv6 address, enable or disable DHCPv6 server and RADVD, and configure site prefix.



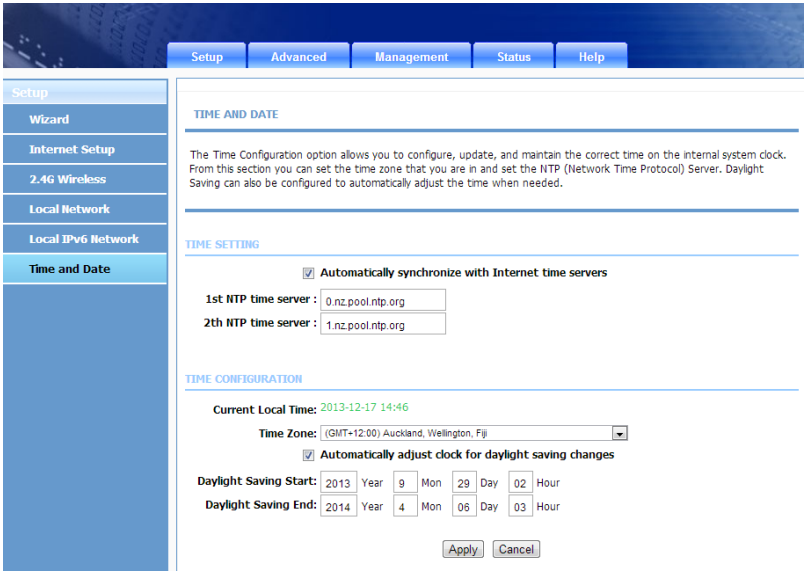
The following table describes the parameters in this page.

Field	Description
IPv6 Address	The IPv6 address of link local gateway on the LAN side.
Enable DHCPv6 Server	Choose to enable DHCPv6 server.
LAN address config mode	Choose an IPv6 address mode. **Stateless** refers to stateless address auto-configuration (SLAAC) mode, and **Stateful** refers to dynamic host configuration protocol (DHCP) mode.
Start/ End Interface ID	IPv6 address pool range.
DHCPv6 Lease Time	IPv6 lease time.
Get DNS Servers from WAN	You can choose to get the IPv6 DNS server address from the WAN side.
Static DNS Servers	You can manually set the IPv6 DNS server address.
Static IPv6 DNS Servers	Input an IPv6 DNS server address.
Enable RADVD	The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.
Auto get prefix from WAN	You can choose to get an IPv6 prefix from the WAN automatically.
WAN interface	You can choose to get an IPv6 prefix from the selected WAN connection.
Static	You can choose to specify an IPv6 prefix.
Site Prefix	Input an IPv6 prefix.

After finishing setting, click the **Apply** button to apply the settings.

5.1.6 Time and Date

Choose **Setup** > **Time and Date**. The page shown in the following figure appears.


Setup
Advanced
Management
Status
Help
Setup
Wizard
Internet Setup
2.4G Wireless
Local Network
Local IPv6 Network
Time and Date
TIME AND DATE
The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.
TIME SETTING
Automatically synchronize with Internet time servers
1st NTP time server : 0.nz.pool.ntp.org
2th NTP time server : 1.nz.pool.ntp.org
TIME CONFIGURATION
Current Local Time: 2013-12-17 14:46
Time Zone: (GMT+12:00) Auckland, Wellington, Fiji
Automatically adjust clock for daylight saving changes
Daylight Saving Start: 2013 Year 9 Mon 29 Day 02 Hour
Daylight Saving End: 2014 Year 4 Mon 06 Day 03 Hour
Apply
Cancel

In the **Time and Date** page, you can configure, update, and maintain the correct time on the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.

Select **Automatically synchronize with Internet time servers**.

Select the specific time server and the time zone from the corresponding drop-down lists.

Select **Automatically adjust clock for daylight saving changes** if necessary.

Set the daylight as you want.

Click **Apply** to save the settings.

5.2 Advanced

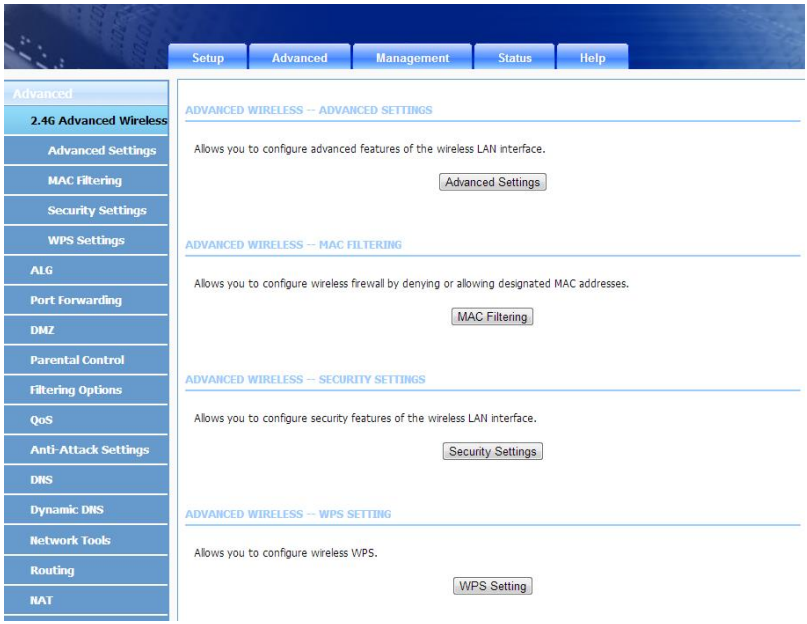
This section includes advanced features for network management, security and administrative tools to manage the device. You can view status and other information used to examine performance and troubleshoot.

In the main interface, click **Advanced** tab to enter the **Advanced** menu as shown in the following figure. The submenus are **Advanced Wireless**, **ALG**, **Port Forwarding**, **DMZ**, **Parental Control**, **Filtering Options**, **QoS Configuration**, **Anti-Attack Settings**, **DNS**, **Dynamic DNS**, **Network Tools**, **Routing**, and **NAT**

Advanced Wireless

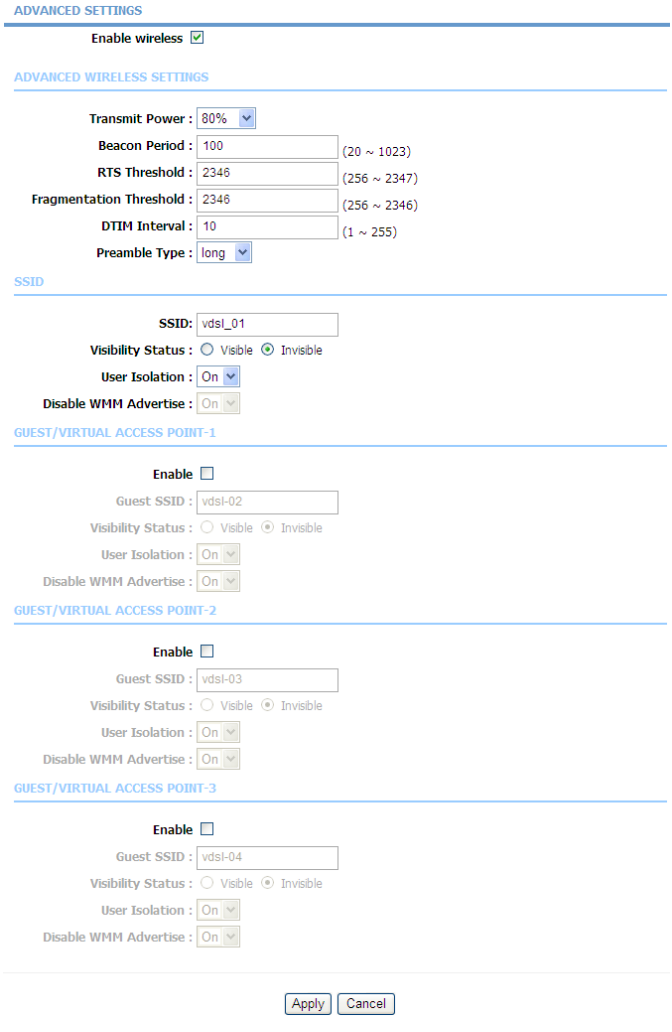
It is suggested not to change the defaults, as incorrect settings may reduce the performance of your wireless radio. The default settings provide the best wireless radio performance in most environments.

Choose **Advanced** > **Advanced Wireless**. The page shown in the following figure appears.



5.2.1.1 Advanced Settings

Select **Advanced Settings**. The page shown in the following figure appears.



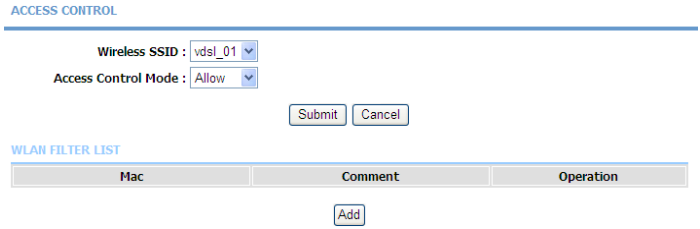
Wireless Network Name (SSID): The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Do not change these settings unless you know the effect of changes on the device.

Click **Apply** to save the settings.

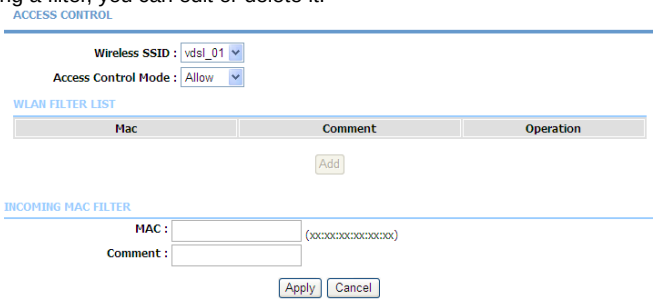
5.2.1.2 MAC Filtering

Select **MAC Filtering**. The page shown in the following figure appears.



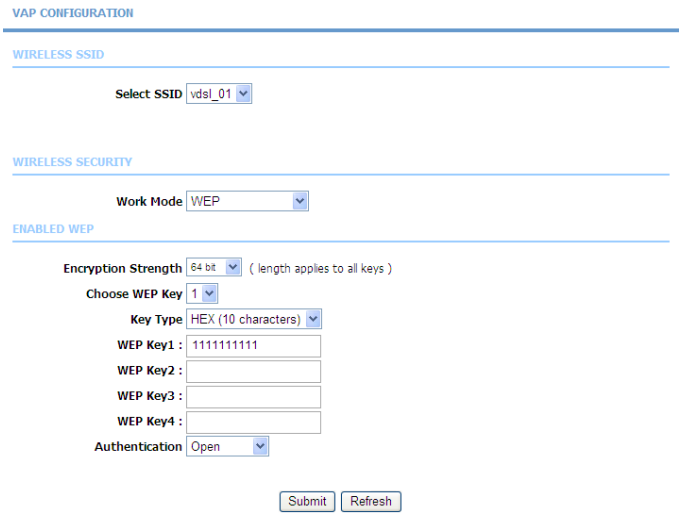
MAC address access control permits access to this route from hosts with MAC addresses contained in the WLAN Filter List.

Choose a wireless SSID, select an access control mode, and then click **Add** to add a MAC Address as shown in the following figure. Click **Apply** to finish. After adding a filter, you can edit or delete it.



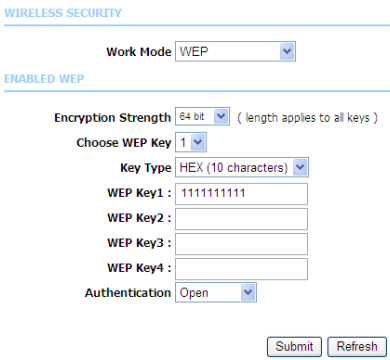
5.2.1.3 Security Settings

Select **Security Settings**. The VAP Configuration page appears.

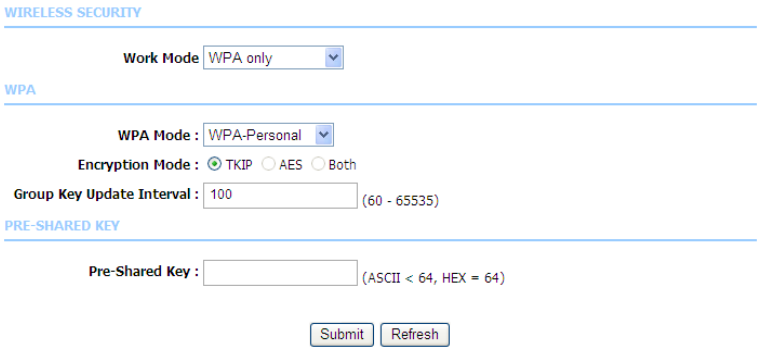


Select the SSID that you want to configure from the drop-down list. Select the encryption type from the **Work Mode** drop-down list. You can select **None**, **WEP**, **WPA Only**, **WPA2 Only** or **WPA/WPA2 Mixed**. The default mode is **None**.

If you select **WEP**, the page shown in the following figure appears.



If you select **WPA Only**, **WPA2 Only** or **WPA/WPA2 Mixed**, the page shown in the following figure appears.



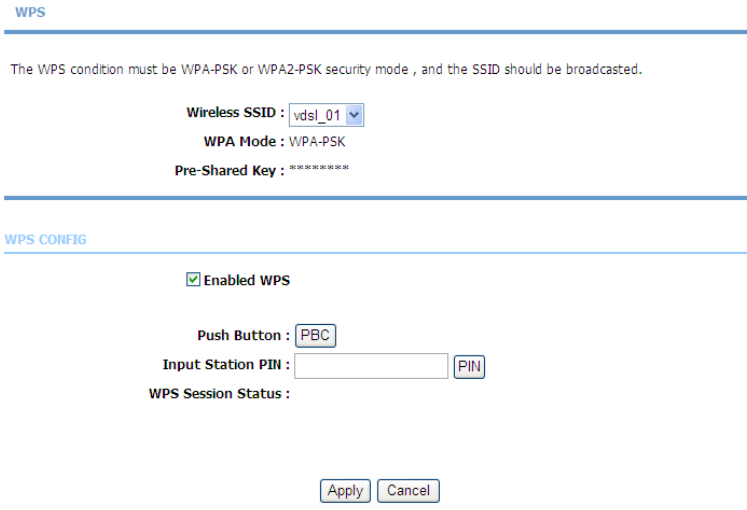
Click **Submit** to save the settings. For detailed configuration, you may refer to 5.1.3.2 Wireless Security.

5.2.1.4 WPS Settings

Select **WPS Settings**. This page is used to config WPS settings.

Note:

To configure WPS, the WLAN security mode must be WPA-PSK or WPA2-PSK mode.


WPS
The WPS condition must be WPA-PSK or WPA2-PSK security mode , and the SSID should be broadcasted.
Wireless SSID : vdsl_01
WPA Mode : WPA-PSK
Pre-Shared Key : ********
WPS CONFIG
Enabled WPS
Push Button : PBC
Input Station PIN : PIN
WPS Session Status :
Apply
Cancel

The following table describes the parameters of this page.

Field	Description
Wireless SSID	Select one SSID of the CPE.
Enabled WPS	Choose to enable WPS function to set the following parameters.
PBC	In this way, the router generates PIN. Click this button, the router will generate a PIN, and meanwhile press the WPS button on the wireless client. The wireless client automatically establishes connection with the router under encryption mode without inputting the key.
PIN	In this way, the wireless client generates PIN. Enter PIN of the wireless client in the **Input Station PIN** field, and then click **PIN** to establish the connection.
WPS Session Status	Display the session status.

5.2.2 ALG

Choose **Advanced** > **ALG**. The page shown in the following figure appears. In this page, you can enable passthrough of TFTP, FTP, PPTP, RTSP, L2TP, H323, SIP and IPSEC.

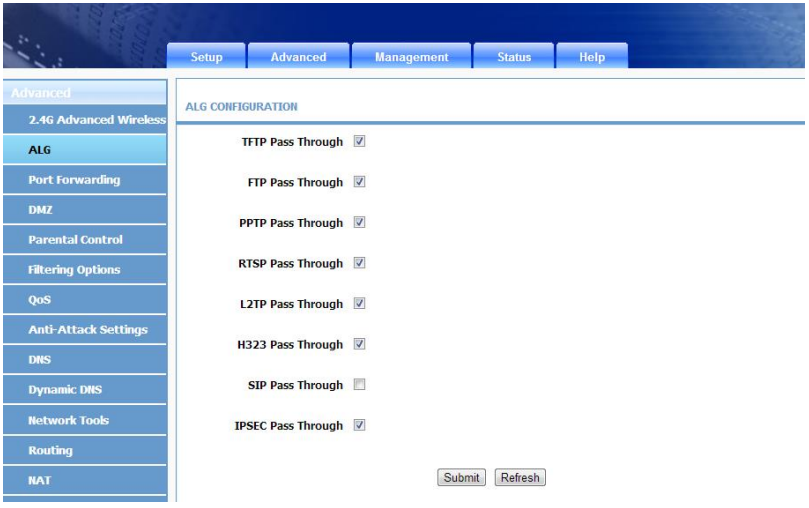
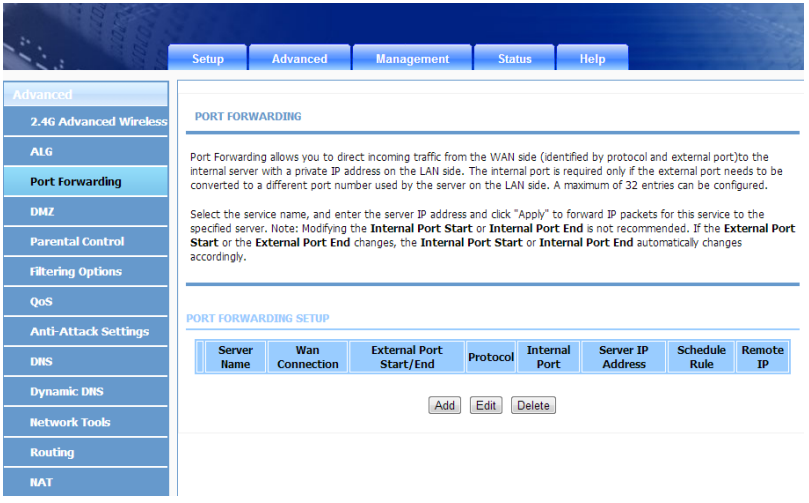


Figure 6

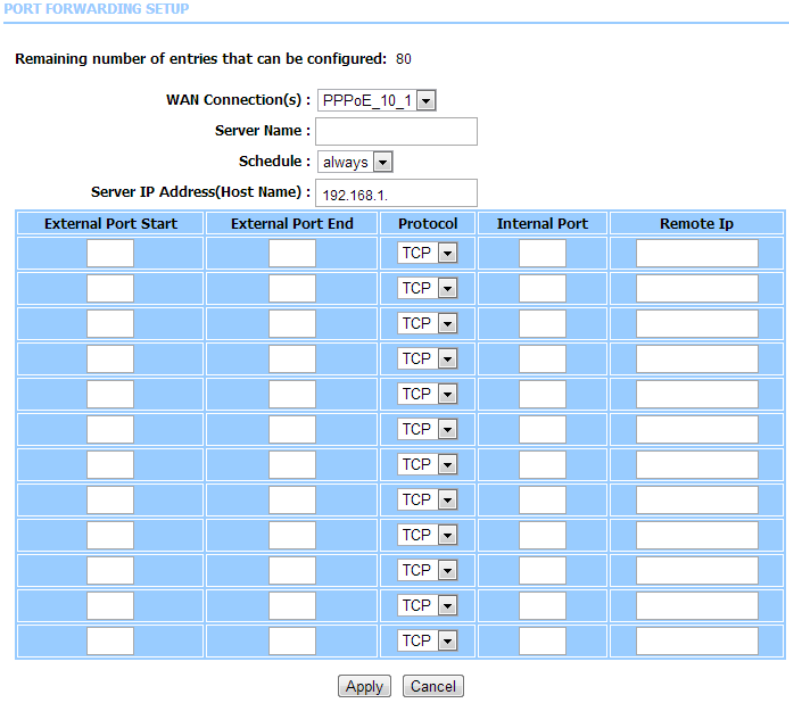
5.2.3 Port Forwarding

This function is used to open ports in your device and redirect data through those ports to a single PC on your network (WAN-to-LAN traffic). It allows remote users to access services on your LAN, such as FTP for file transfers or SMTP and POP3 for e-mail. The device accepts remote requests for these services at your global IP address. It uses the specified TCP or UDP protocol and port number, and redirects these requests to the server on your LAN with the LAN IP address you specify. Note that the specified private IP address must be within the available range of the subnet where the device is in.

Choose **Advanced** > **Port Forwarding**. The page shown in the following figure appears.


Setup
Advanced
Management
Status
Help
Advanced
2.4G Advanced Wireless
ALG
Port Forwarding
DMZ
Parental Control
Filtering Options
QoS
Anti-Attack Settings
DNS
Dynamic DNS
Network Tools
Routing
NAT
PORT FORWARDING
Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port)to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.
Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the Internal Port Start or Internal Port End is not recommended. If the External Port Start or the External Port End changes, the Internal Port Start or Internal Port End automatically changes accordingly.
PORT FORWARDING SETUP
Server Name
Wan Connection
External Port Start/End
Protocol
Internal Port
Server IP Address
Schedule Rule
Remote IP
Add
Edit
Delete

Click **Add** to add a virtual server.



Enter a name in the **Server Name** field.

Enter an IP address in the **Server IP Address** field to appoint the corresponding PC to receive forwarded packets.

Enter an External Port start and end range, and select Protocol type.

Click **Apply** to save the settings. The page shown in the following figure appears. A virtual server is added.

PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port)to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

PORT FORWARDING SETUP

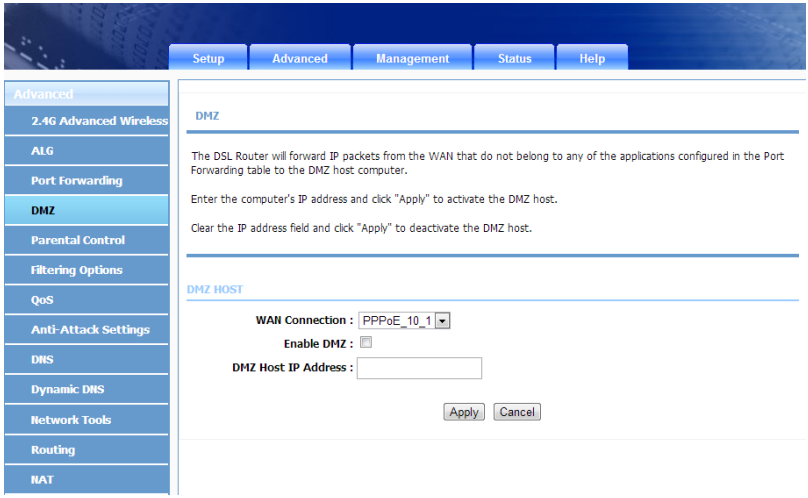
	Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP
☐	Active W...	PVC:8/32	3000/3000	tcp	3000/3000	192.168.1.10	Always	
☐	Active W...	PVC:8/32	5670/5670	tcp	5670/5670	192.168.1.10	Always	
☐	Active W...	PVC:8/32	7777/7777	tcp	7777/7777	192.168.1.10	Always	
☐	Active W...	PVC:8/32	7000/7000	tcp	7000/7000	192.168.1.10	Always	

Add Edit Delete

5.2.4 DMZ

Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

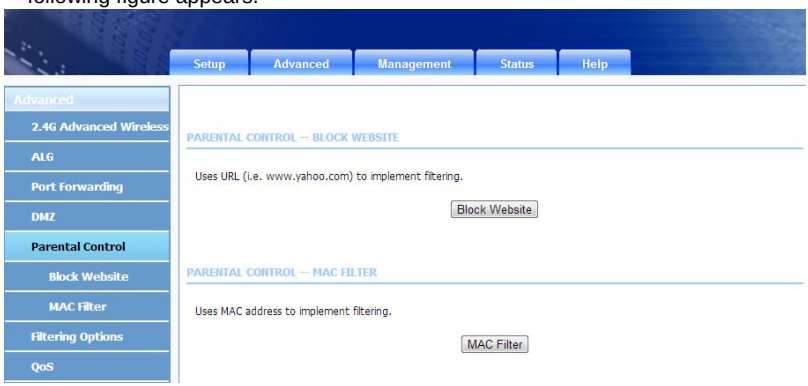
Choose **Advanced** > **DMZ**. The page shown in the following figure appears.



Choose to enable DMZ, input a DMZ host ip address, and click then **Apply** to save the settings.

5.2.5 Parental Control

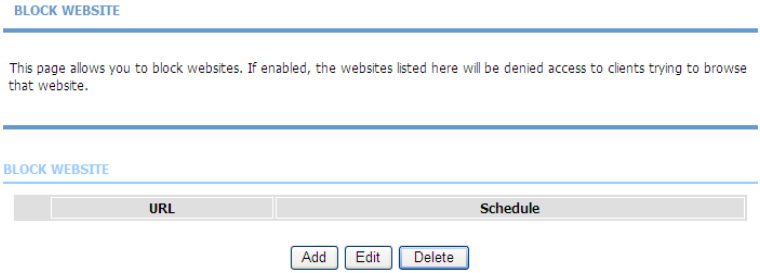
Choose **Advanced** > **Parental Control**. The **Parent Control** page shown in the following figure appears.



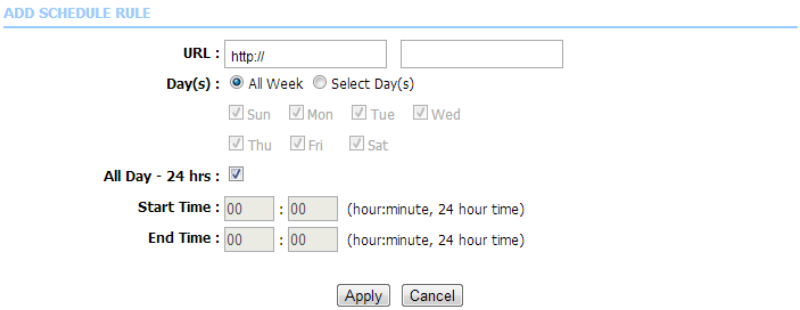
This page provides two useful tools for restricting the Internet access. **Block Websites** allows you to quickly create a list of all websites that you wish to stop users from accessing. **MAC Filter** allows you to control when clients or PCs connected to the device are allowed to access the Internet.

5.2.5.1 Block Website

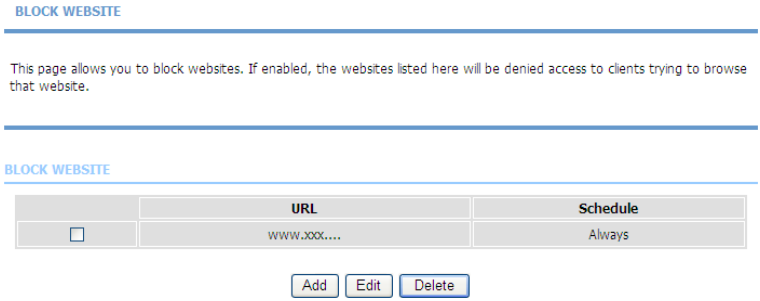
In the **Parental Control** page, click **Block Website**. The page shown in the following figure appears.


BLOCK WEBSITE
This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.
BLOCK WEBSITE
URL
Schedule
Add
Edit
Delete

Click **Add**. The page shown in the following figure appears.

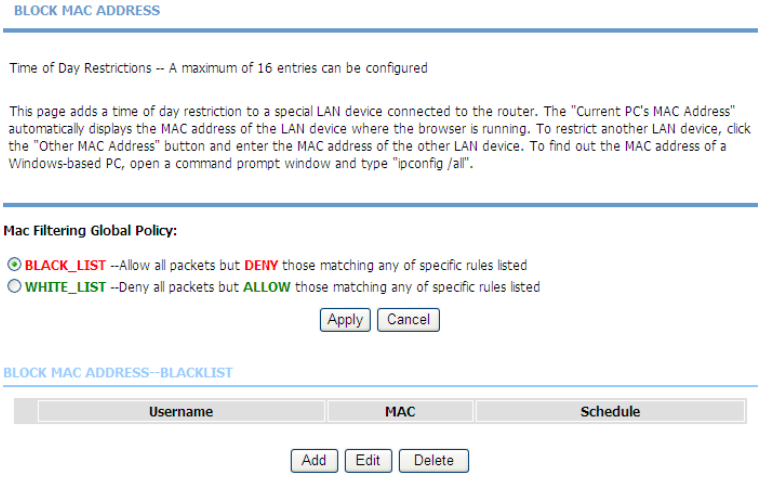

ADD SCHEDULE RULE
URL : http://
Day(s) : All Week Select Day(s)
Sun Mon Tue Wed
Thu Fri Sat
All Day - 24 hrs :
Start Time : 00 : 00 (hour:minute, 24 hour time)
End Time : 00 : 00 (hour:minute, 24 hour time)
Apply
Cancel

Enter the website in the **URL** field. Select the corresponding time and days. Click **Apply** to add the website to the **BLOCK WEBSITE** table. The page shown in the following figure appears.

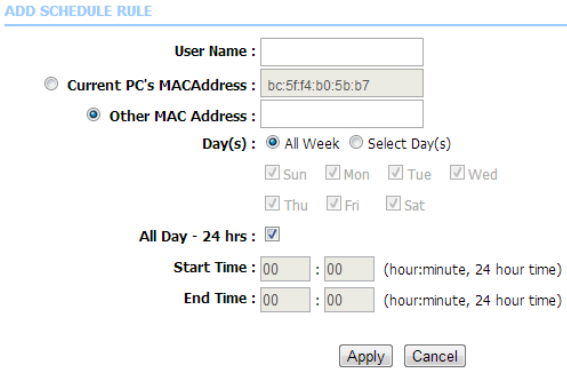


5.2.5.2 MAC Filter

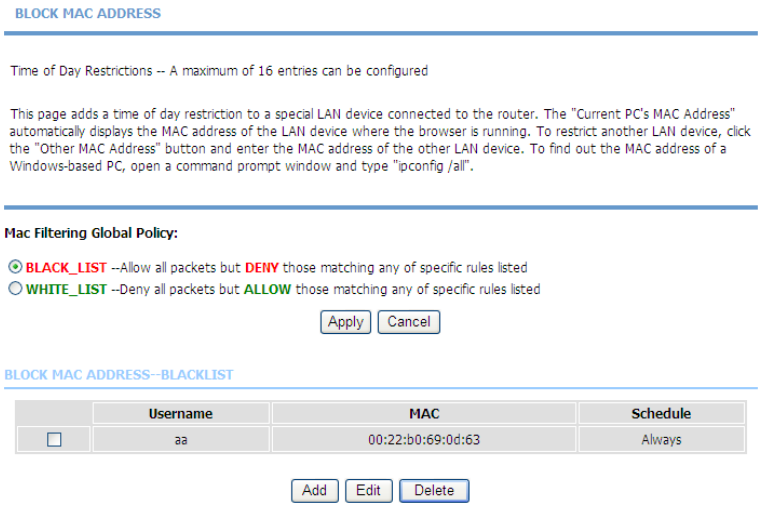
In the **Parental Control** page, click **MAC Filter**. The page shown in the following figure appears.


BLOCK MAC ADDRESS
Time of Day Restrictions -- A maximum of 16 entries can be configured
This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".
Mac Filtering Global Policy:
BLACK_LIST --Allow all packets but DENY those matching any of specific rules listed
WHITE_LIST --Deny all packets but ALLOW those matching any of specific rules listed
Apply
Cancel
BLOCK MAC ADDRESS--BLACKLIST
Username
MAC
Schedule
Add
Edit
Delete

Choose **BLACK_LIST** or **WHITE_LIST**, and then click **Add**. The page shown in the following figure appears.

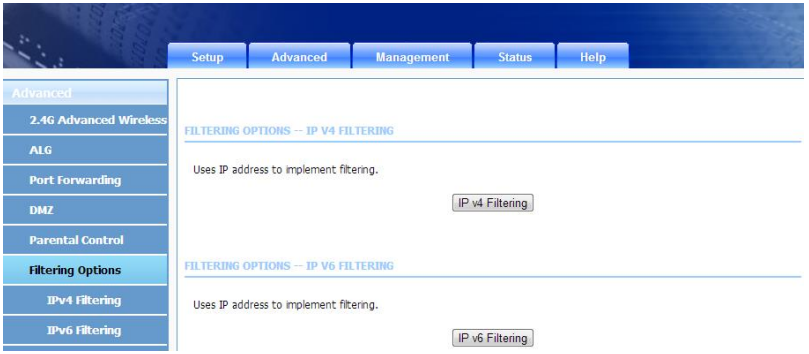

ADD SCHEDULE RULE
User Name :
Current PC's MACAddress : bc:5f:f4:b0:5b:b7
Other MAC Address :
Day(s) : All Week Select Day(s)
Sun Mon Tue Wed
Thu Fri Sat
All Day - 24 hrs :
Start Time : 00 : 00 (hour:minute, 24 hour time)
End Time : 00 : 00 (hour:minute, 24 hour time)
Apply Cancel

Enter the use name and MAC address and select the corresponding time and days. Click **Apply** to add the MAC address to the **BLOCK MAC ADDRESS Table**. The page shown in the following figure appears.


BLOCK MAC ADDRESS
Time of Day Restrictions -- A maximum of 16 entries can be configured
This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".
Mac Filtering Global Policy:
BLACK_LIST --Allow all packets but DENY those matching any of specific rules listed
WHITE_LIST --Deny all packets but ALLOW those matching any of specific rules listed
Apply Cancel
BLOCK MAC ADDRESS--BLACKLIST
Username MAC Schedule
aa 00:22:b0:69:0d:63 Always
Add Edit Delete

5.2.6 Filtering Options

Choose **Advanced** > **Filtering Options**. The **Filtering Options** page shown in the following figure appears.

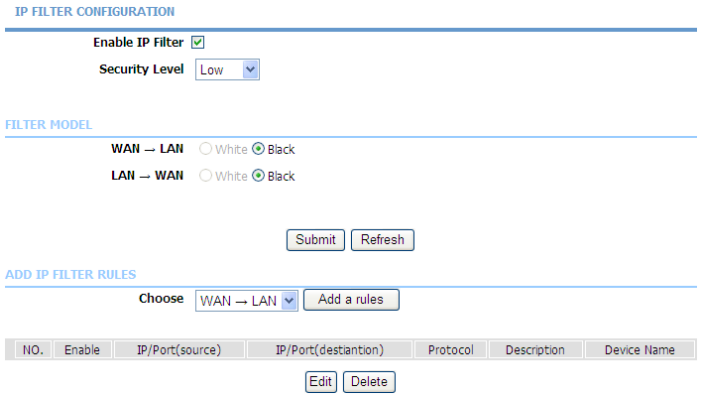


5.2.6.1 IPv4 Filtering

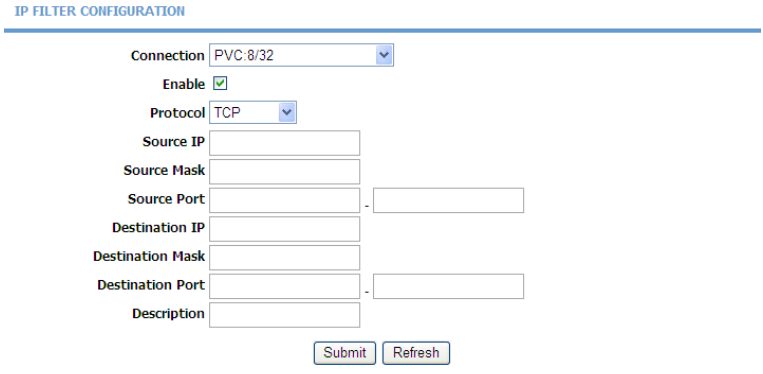
In the **Filtering Options** page, click **IPv4 Filtering**. The page shown in the following figure appears. In this page, you may configure IPv4 firewall function.

Note:

The settings are applicable only when IP filter is enabled.



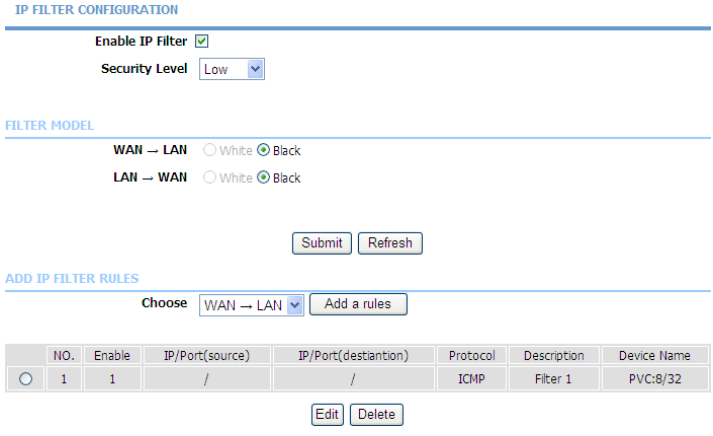
Select a security level, choose a filter direction, and then click **Add a rule** to display the following figure.



The following table describes the parameters of this page.

Field	Description
Connection	Choose an IPv4 WAN connection.
Enable	Tick in the box to enable a filter rule.
Protocol	Choose a protocol corresponding to the rule. You may choose **TCP**, **UDP**, **ICMP** or **TCP/UDP**.
Source/ Destination IP	Original/ destination IP address.
Source/ Destination Mask	Original/ destination mask.
Source/Destination Port	Original/ end port, which is the original port range.
Description	You can describe this IPv4 filter rule.

After setting the parameters, click **Submit**. The page shown in the following figure appears. You can also click **Edit** or **Delete** to manage the rule.

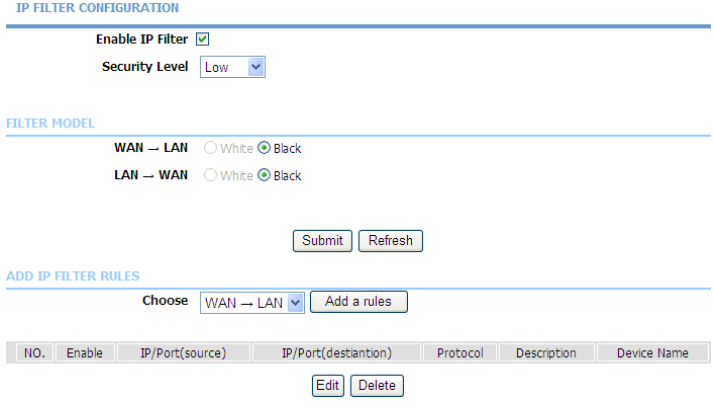


5.2.6.2 IPv6 Filtering

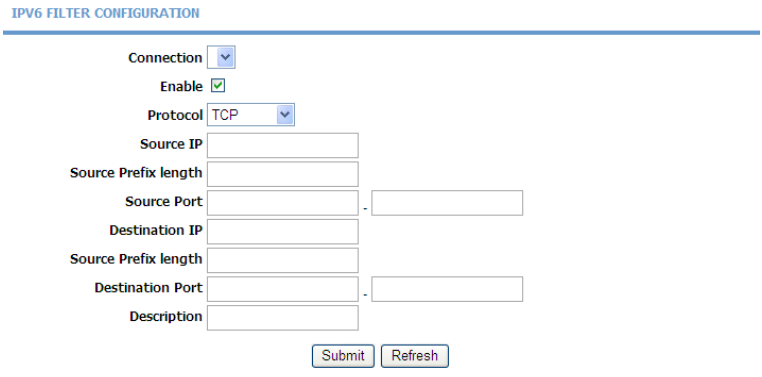
In the **Filtering Options** page, click **IPv6 Filtering**. The page shown in the following figure appears. In this page, you may configure IPv6 firewall function.

Note:

The settings are applicable only when the firewall is enabled.



Select a security level, choose a filter direction, and then click **Add a rule** to display the following figure.



The following table describes the parameters of this page.

Field	Description
Connection	Choose an IPv6 WAN connection.
Enable	Tick in the box to enable a firewall rule.
Protocol	Choose a protocol corresponding to the rule. You may choose **TCP**, **UDP**, **ICMPv6** or **TCP/UDP**.
Source/ Destination IP	Original/ destination IP address
Source prefix length	Original/ destination mask
Source/Destination Port	Original/ end port, which is the original port range
Description	You can describe this IPv6 filter rule.

After setting the parameters, click **Submit**. The page shown in the following figure appears. You can also click **Edit** or **Delete** to manage the rule.

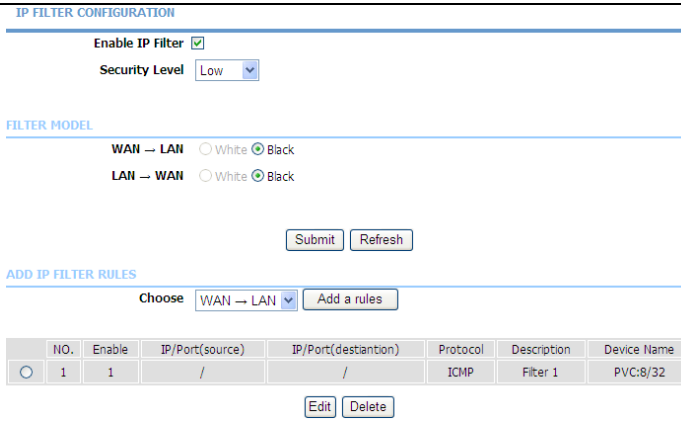

IP FILTER CONFIGURATION
Enable IP Filter
Security Level
Low
FILTER MODEL
WAN → LAN
White
Black
LAN → WAN
White
Black
Submit
Refresh
ADD IP FILTER RULES
Choose
WAN → LAN
Add a rules
NO.
Enable
IP/Port(source)
IP/Port(destiantion)
Protocol
Description
Device Name
1
1
/
/
ICMP
Filter 1
PVC:8/32
Edit
Delete

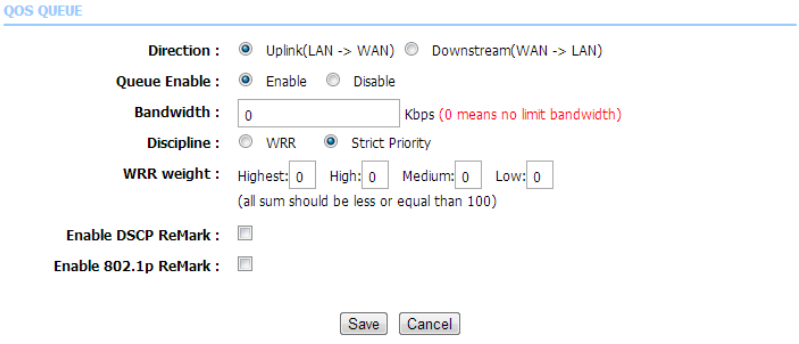
Figure 7

5.2.7 QoS Configuration

Choose **Advanced** > **QoS**. The **QoS Configuration** page shown in the following figure appears.

5.2.7.1 QoS Queue Config

In the **QoS Configuration** page, enable **QoS**. The page shown in the following figure appears. In this page, you can set QoS flow control.

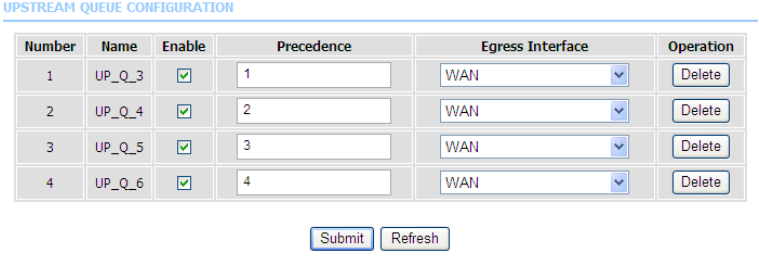


The following table describes the parameters of this page.

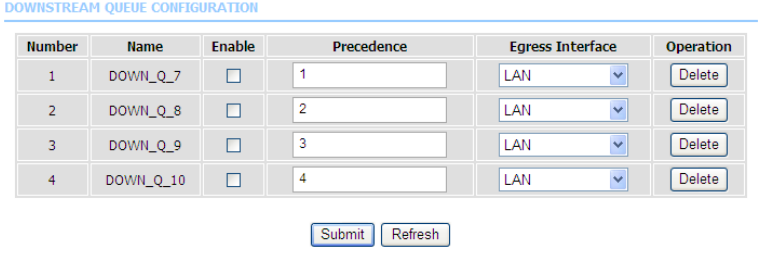
Field	Description
Direction	Choose **Upstream** queue or **Downstream** queue.
Enable	Tick in the box to enable queue.
Bandwidth	Total bandwidth
Enable DSCP/TC Mark	You may tick in the box to permit DSCP/TC Mark.
Enable 802.1P Mark	You may tick in the box to permit 802.1P Mark.

After setting the parameters, click **Add Queue** to add a queue.

In the above page, when **Upstream (Lan -> Wan)** direction is chosen, you need to configure the parameters in the following figure.



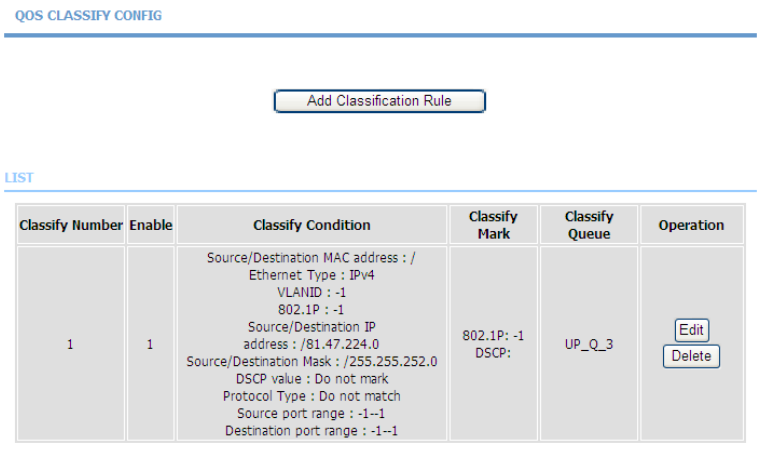
When **Downstream (Lan -> Wan)** direction is chosen, you need to configure the parameters in the following figure.



After modifying a queue, click **Submit** to enable the modification. Click **Refresh** to refresh the queue.

5.2.7.2 QoS Classification

In the **QoS Configuration** page, the page shown in the following figure appears. You can configure QoS queue rule.



Click **Add Classification Rule**. The page shown in the following figure appears.

The following table describes the parameters of this page.

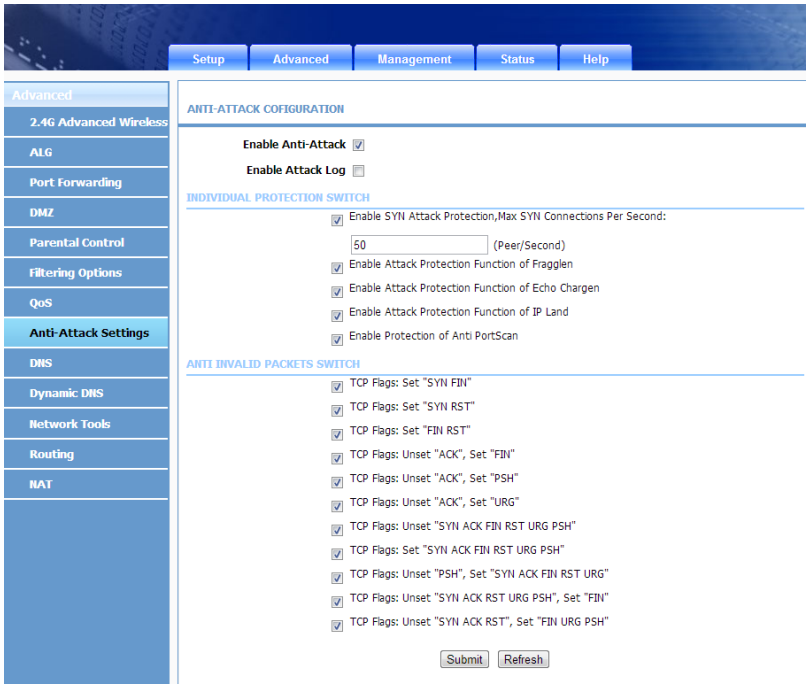
Field	Description
Classify Type	Set the QoS rule type as **Upstream** or **Downstream**.
Active	Select enable to enable this QoS rule.
Input Interface	Based on the Classify Type, choose a WAN/LAN interface.

Field	Description
802.1P	Choose a matched 802.1P VLAN priority.
DSCP Check	Choose a matched DSCP type.
Protocol Type	Choose a protocol type matching with the QoS rule.
Source/ Destination port range	Input a source port range and a destination port range. For example, input a UDP/TCP port range.
Classify Queue	Choose a QoS queue for the rule.
DSCP Mark	Set a DSCP Mark for this QoS rule.

Click Submit to add the rule to the list. You may click **Edit** to modify the existing classification rule, or click **Delete** to delete it.

5.2.8 Anti-Attack Settings

Choose **Advanced** > **Anti-Attack Settings**. The **Anti-Attack Configuration** page shown in the following figure appears.



A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

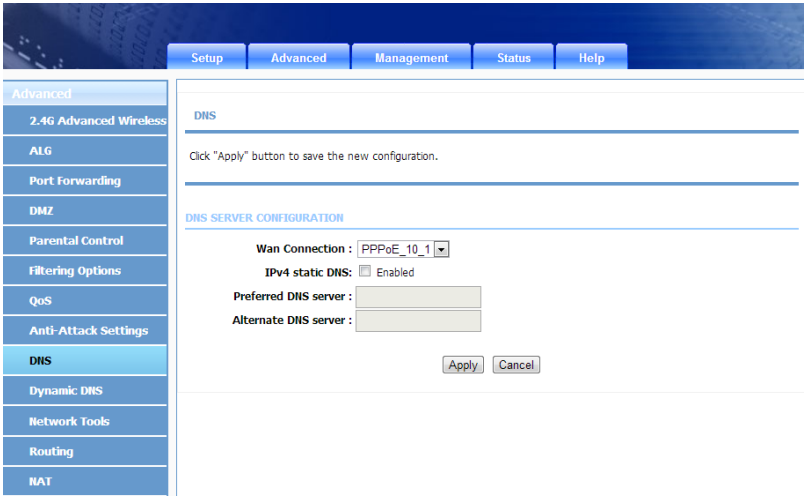
Click **Submit** to save the settings.

5.2.9 DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **Advanced** > **DNS**. The page shown in the folllowing figure appears.



If you are using the device for DHCP service on the LAN or using DNS servers on the ISP network, select **Obtain DNS server address automatically**.

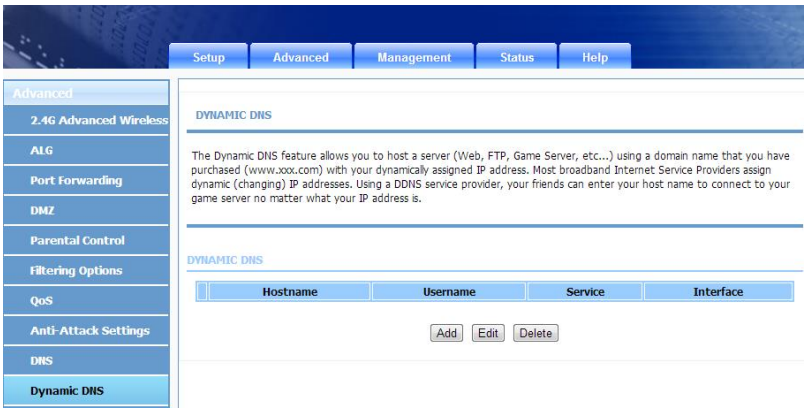
If you have DNS IP addresses provided by your ISP, select **Use the following DNS server addresses**, and enter these IP addresses in the available entry fields for the preferred DNS server and the alternate DNS server.

Click **Apply** to save the settings.

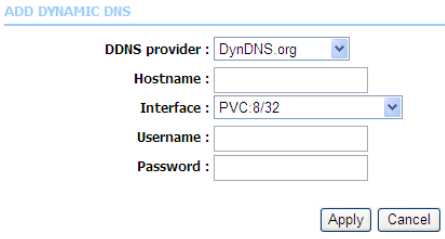
5.2.10 Dynamic DNS

The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of hostname.dyndns.org and allow remote access to a host. Many ISPs assign public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers (DyndDNS.org, 3322.org and freedns.afraid.org).

Choose **Advanced** > **Dynamic DNS**. The page shown in the following figure appears.



Click **Add** to add dynamic DNS. The page shown in the following figure appears.



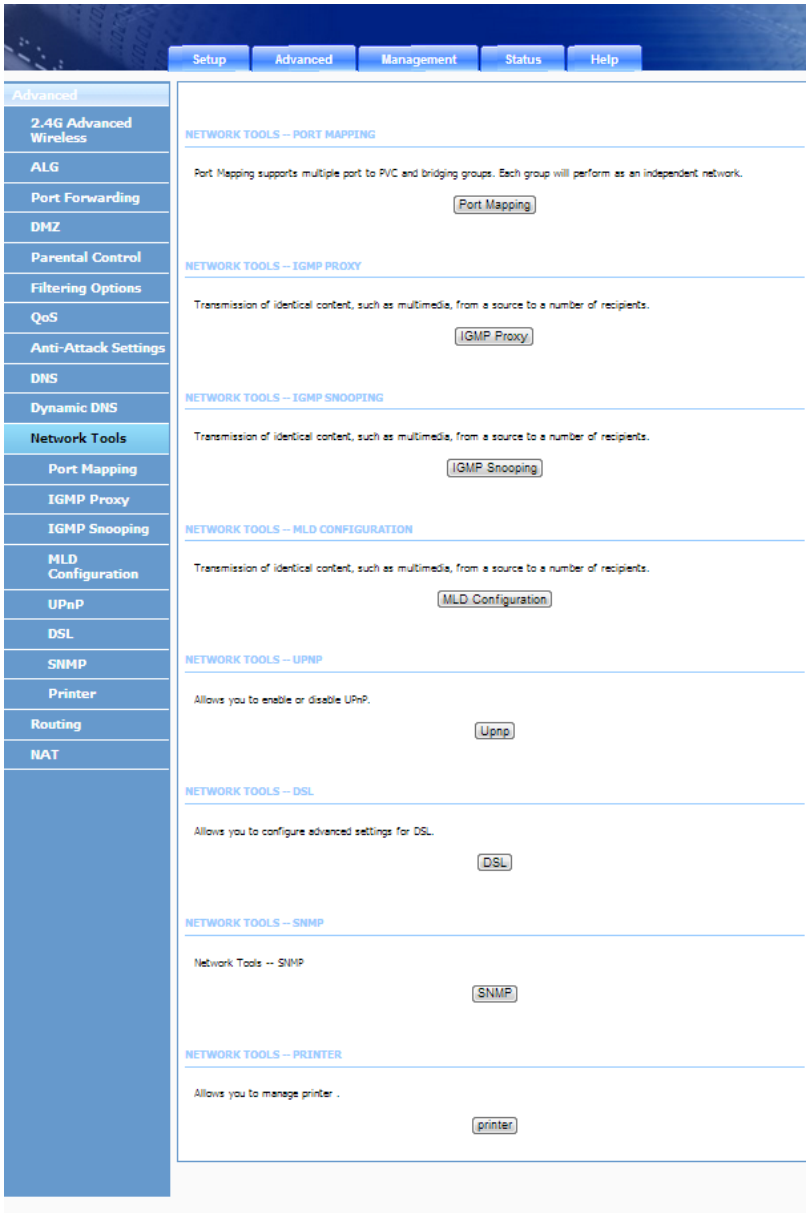
The following table describes the parameters of this page.

Field	Description
DDNS provider	Select one of the DDNS registration organizations from the down-list drop. Available servers include **DynDns.org**, **3322.org** and **freedns.afraid.org**.
Host Name	Enter the host name that you registered with your DDNS service provider.
Username	Enter the user name for your DDNS account.
Password	Enter the password for your DDNS account.

Click **Apply** to save the settings.

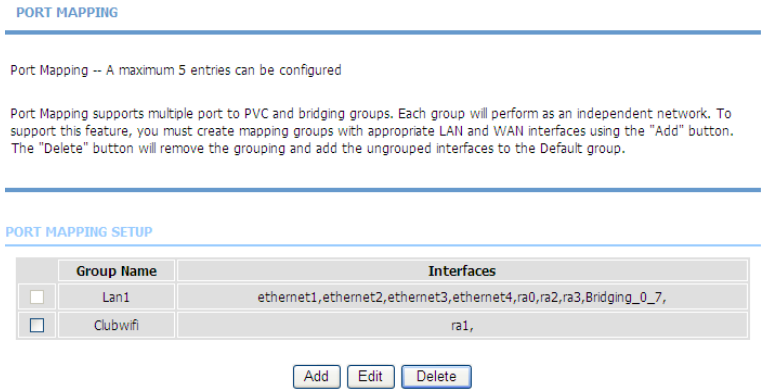
5.2.11 Network Tools

Choose **Advanced** > **Network Tools**. The page shown in the following figure appears.

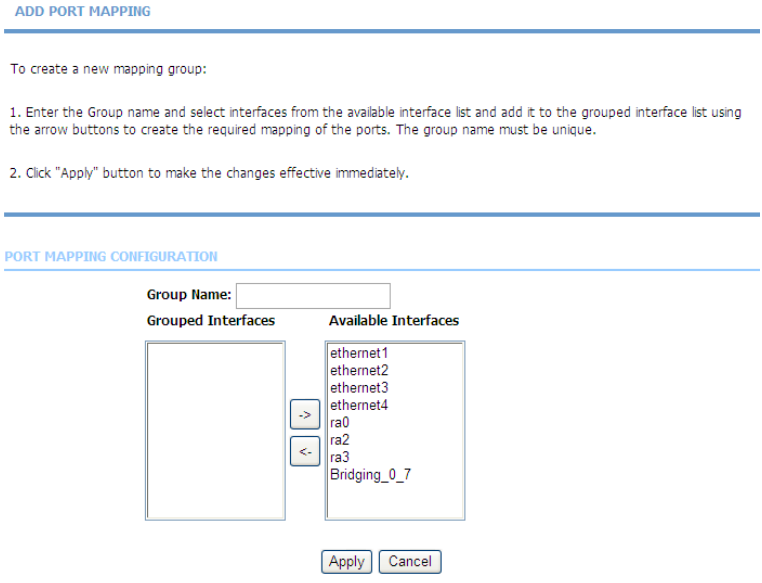

Setup
Advanced
Management
Status
Help
Advanced
2.4G Advanced Wireless
ALG
Port Forwarding
DMZ
Parental Control
Filtering Options
QoS
Anti-Attack Settings
DNS
Dynamic DNS
Network Tools
Port Mapping
IGMP Proxy
IGMP Snooping
MLD Configuration
UPnP
DSL
SNMP
Printer
Routing
NAT
NETWORK TOOLS -- PORT MAPPING
Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.
Port Mapping
NETWORK TOOLS -- IGMP PROXY
Transmission of identical content, such as multimedia, from a source to a number of recipients.
IGMP Proxy
NETWORK TOOLS -- IGMP SNOOPING
Transmission of identical content, such as multimedia, from a source to a number of recipients.
IGMP Snooping
NETWORK TOOLS -- MLD CONFIGURATION
Transmission of identical content, such as multimedia, from a source to a number of recipients.
MLD Configuration
NETWORK TOOLS -- UPNP
Allows you to enable or disable UPnP.
Upnp
NETWORK TOOLS -- DSL
Allows you to configure advanced settings for DSL.
DSL
NETWORK TOOLS -- SNMP
Network Tools -- SNMP
SNMP
NETWORK TOOLS -- PRINTER
Allows you to manage printer .
printer

5.2.11.1 Port Mapping

Choose **Advanced** > **Network Tools** and click **Port Mapping**. The page shown in the following figure appears. In this page, you can bind the WAN interface and the LAN interface to the same group.


PORT MAPPING
Port Mapping -- A maximum 5 entries can be configured
Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.
PORT MAPPING SETUP
Group Name
Interfaces
Lan1
ethernet1,ethernet2,ethernet3,ethernet4,ra0,ra2,ra3,Bridging_0_7,
Clubwifi
ra1,
Add
Edit
Delete

Click **Add** to add port mapping. The page shown in the following figure appears.


ADD PORT MAPPING
To create a new mapping group:
1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. Click "Apply" button to make the changes effective immediately.
PORT MAPPING CONFIGURATION
Group Name:
Grouped Interfaces
Available Interfaces
ethernet1
ethernet2
ethernet3
ethernet4
ra0
ra2
ra3
Bridging_0_7
->
<-
Apply
Cancel

The procedure for creating a mapping group is as follows:

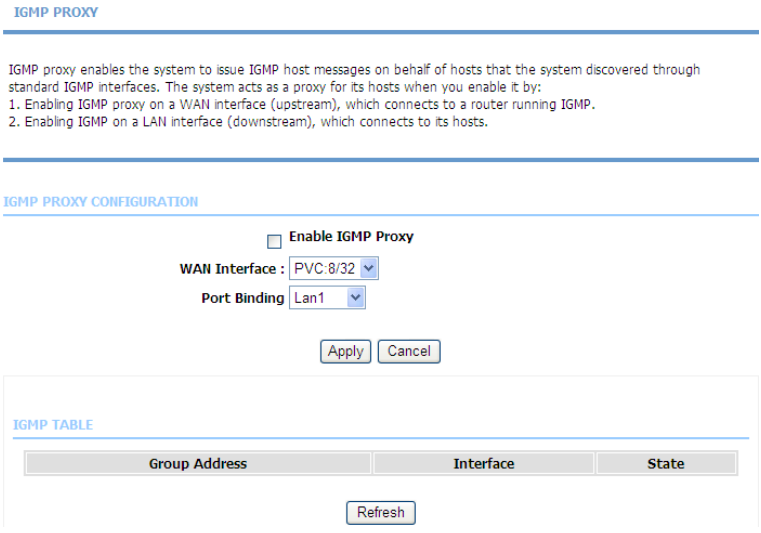
Step 1 Enter the group name.

Step 2 Select interfaces from the **Available Interface** list and click the **<-** arrow button to add them to the grouped interface list, in order to create the required mapping of the ports. The group name must be unique.

Step 3 Click **Apply** to save the settings.

5.2.11.2 IGMP Proxy

Choose **Advanced** > **Network Tools** and click **IGMP Proxy**. The page shown in the following figure appears.


IGMP PROXY
IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by:
1. Enabling IGMP proxy on a WAN interface (upstream), which connects to a router running IGMP.
2. Enabling IGMP on a LAN interface (downstream), which connects to its hosts.
IGMP PROXY CONFIGURATION
Enable IGMP Proxy
WAN Interface : PVC:8/32
Port Binding Lan1
Apply
Cancel
IGMP TABLE
Group Address
Interface
State
Refresh

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.

Click **Apply** to save the settings.

5.2.11.3 IGMP Snooping

Choose **Advanced** > **Network Tools** and click **IGMP Snooping**. The page shown in the following figure appears. When IGMP Snooping is enabled, the multicast data transmits through the specific LAN port which has received the request report.

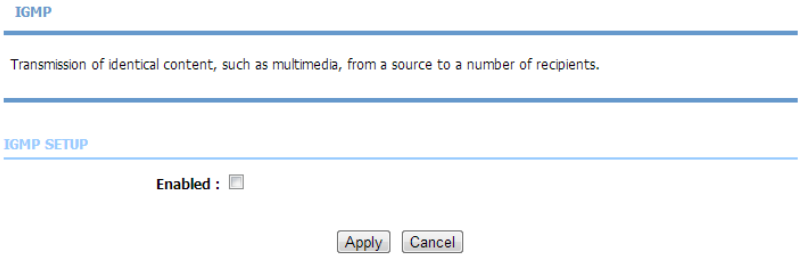
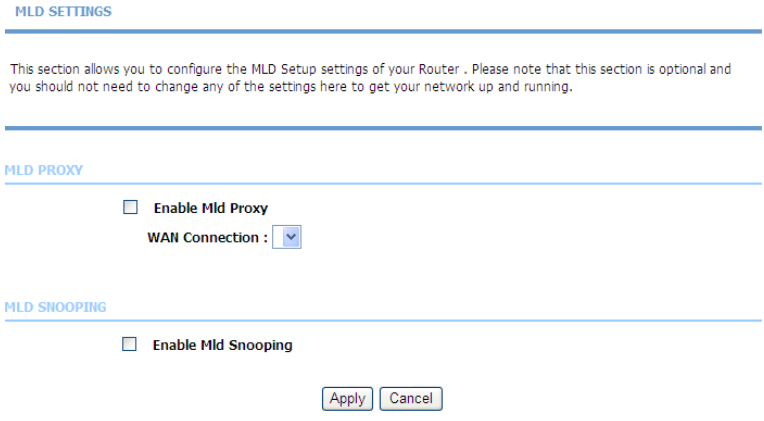

IGMP
Transmission of identical content, such as multimedia, from a source to a number of recipients.
IGMP SETUP
Enabled :
Apply
Cancel

Figure 8

5.2.11.4 MLD Configuration

Choose **Advanced** > **Network Tools** and click **MLD Configuration**. The page shown in the following figure appears. This section allows you to configure the MLD setup settings of your router.

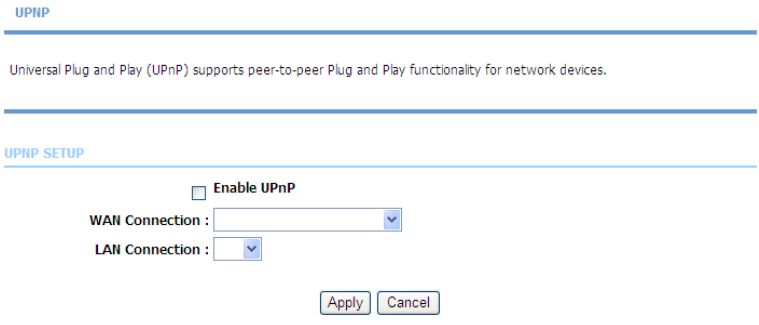

MLD SETTINGS
This section allows you to configure the MLD Setup settings of your Router . Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.
MLD PROXY
Enable Mld Proxy
WAN Connection :
MLD SNOOPING
Enable Mld Snooping
Apply
Cancel

The following table describes the parameters of this page.

Field	Description
Enable Mld Proxy	You can choose to enable MLD proxy.
WAN Connection	Choose an IPv6 WAN connection.
Enable MLD Snooping	Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

5.2.11.5 UPnP

Choose **Advanced** > **Network Tools** and click **UPnP**. The page shown in the following figure appears.



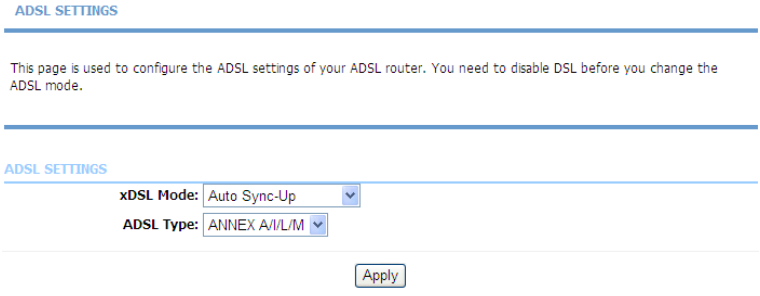
In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

Click **Apply** to save the settings.

5.2.11.6 DSL

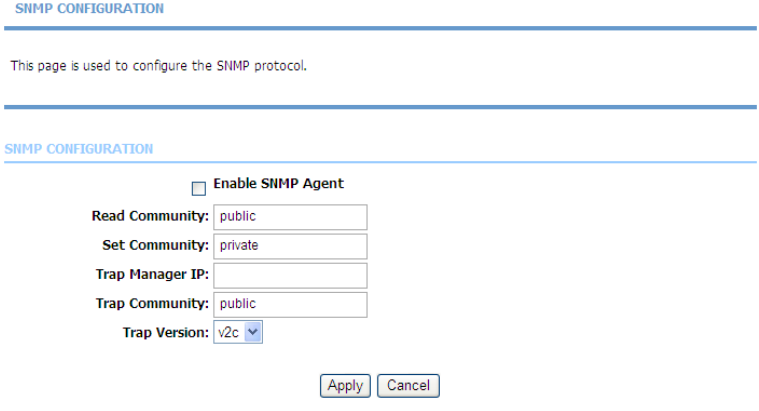
Choose **Advanced** > **Network Tools** and click **DSL**. The page shown in the following figure appears.


ADSL SETTINGS
This page is used to configure the ADSL settings of your ADSL router. You need to disable DSL before you change the ADSL mode.
ADSL SETTINGS
xDSL Mode: Auto Sync-Up
ADSL Type: ANNEX A/I/L/M
Apply

In this page, you can select a DSL mode. Normally, you can keep this factory default setting. The device negotiates the modulation mode with DSLAM.
Click **Apply** to save the settings.

5.2.11.7 SNMP

Choose **Advanced** > **Network Tools** and click **SNMP**. The page shown in the following figure appears. In this page, you can set SNMP parameters.



Click **Apply** to save the settings.

5.2.11.8 Printer

Choose **Advanced** > **Network Tools** and click **Printer**. The **Printer** page shown in the following figure appears. In this page, you can enable/disable printer support.

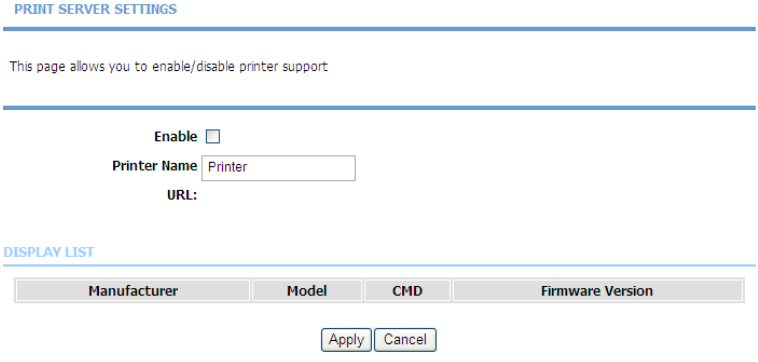


Figure 9

5.2.12 Routing

Choose **Advanced** > **Routing**. The page shown in the following figure appears.

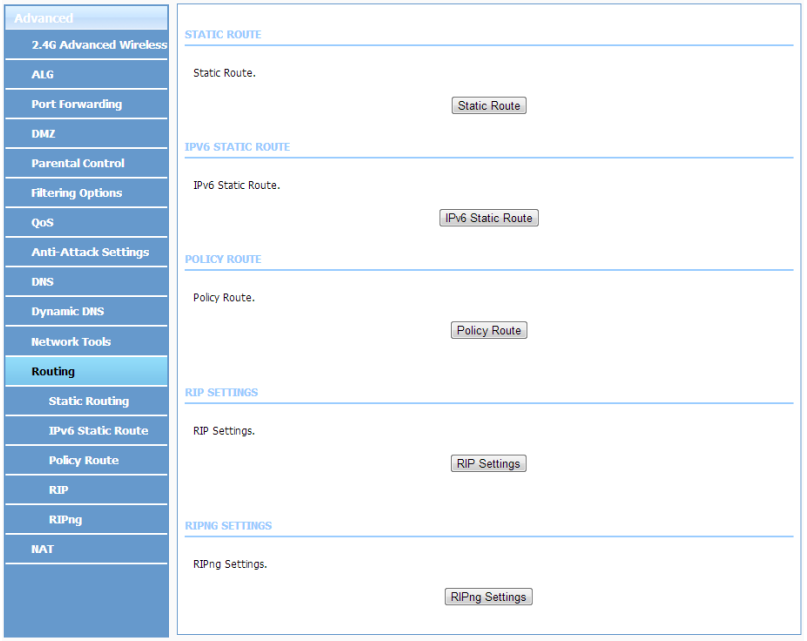
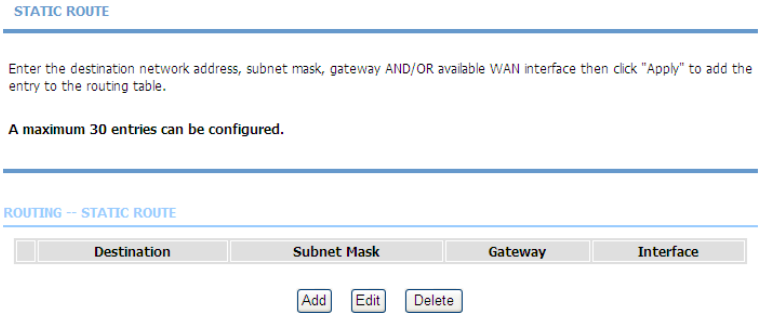


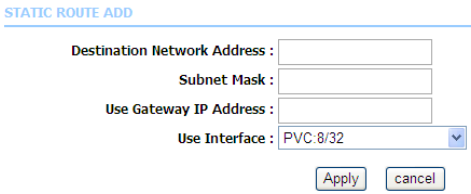
Figure 10

5.2.12.1 Static Routing

Choose **Advanced** > **Routing** and click **Static Routing**. The page shown in the following figure appears. This page is used to configure the routing information. In this page, you can add or delete IP routes.


STATIC ROUTE
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.
A maximum 30 entries can be configured.
ROUTING -- STATIC ROUTE
Destination
Subnet Mask
Gateway
Interface
Add
Edit
Delete

Click **Add** to add a static route. The page shown in the following figure appears.



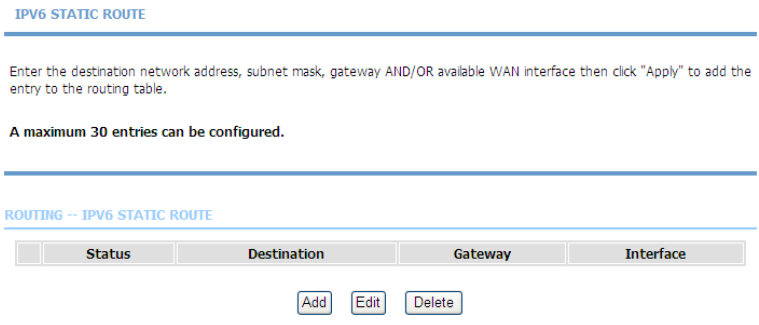
The following table describes the parameters of this page.

Field	Description
Destination Network Address	The destination IP address of the router.
Subnet Mask	The subnet mask of the destination IP
Use Interface	The interface name of the router output port.
Use Gateway IP Address	The gateway IP address of the router.

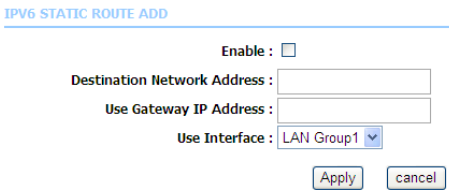
Click **Apply** to save the settings.

5.2.12.2 IPv6 Static Route

Choose **Advanced** > **Routing** and click **IPv6 Static Route**. The page shown in the following figure appears.


IPV6 STATIC ROUTE
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.
A maximum 30 entries can be configured.
ROUTING -- IPV6 STATIC ROUTE
Status
Destination
Gateway
Interface
Add
Edit
Delete

Click Add to add an IPv6 static route. The page shown in the following figure appears.

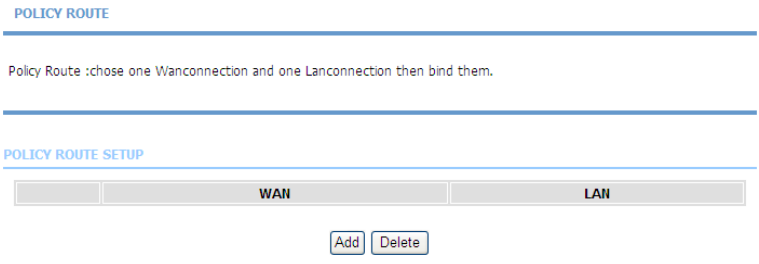


The following table describes the parameters of this page.

Field	Description
Destination Network Address	The destination IP address of the static route.
Use Gateway IP Address	The gateway IP address of the static route.
Use Interface	The interface name of the static route.

5.2.12.3 Policy Route

Choose **Advanced** > **Routing** and click **Policy Route**. The page shown in the following figure appears. The policy route binds one WAN connection and one LAN interface.



Click **Add**, and the page shown in the following figure appears. Choose one WAN connection and at lease one LAN connection to bind together, and then click **Apply**.

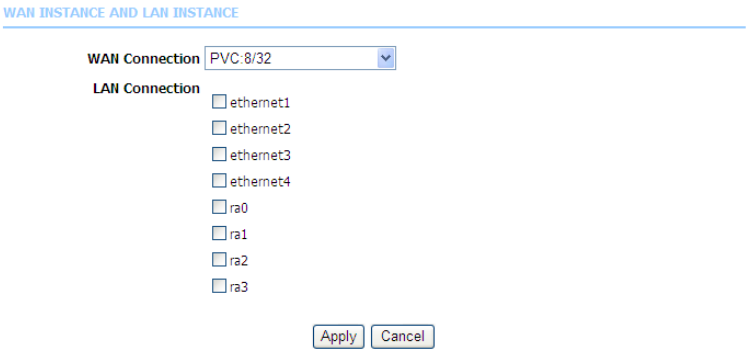
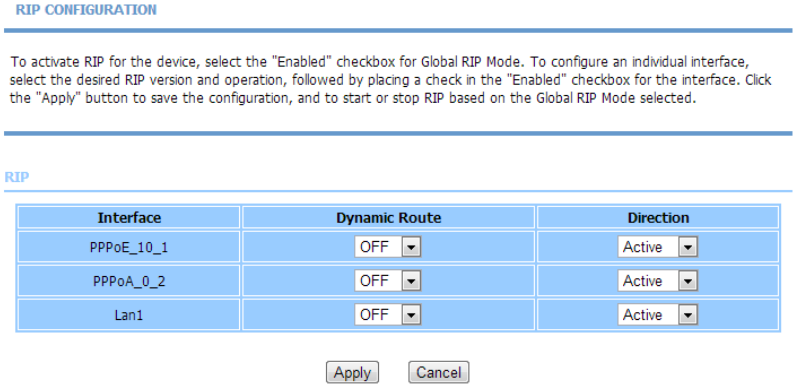


Figure 11

5.2.12.4 RIP

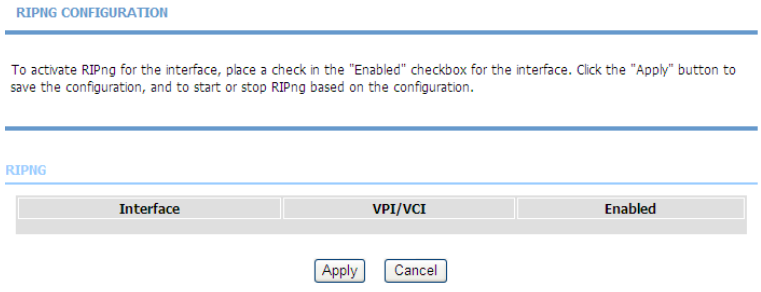
Choose **Advanced** > **Routing** and click **RIP**. The page shown in the following figure appears. This page is used to select the interfaces on your device that use RIP and the version of the protocol used.


RIP CONFIGURATION
To activate RIP for the device, select the "Enabled" checkbox for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIP based on the Global RIP Mode selected.
RIP
Interface
Dynamic Route
Direction
PPPoE_10_1
OFF
Active
PPPoA_0_2
OFF
Active
Lan1
OFF
Active
Apply
Cancel

If you are using this device as a RIP-enabled device to communicate with others using the routing information protocol, enable RIP and click **Apply** to save the settings.

5.2.12.5 RIPng

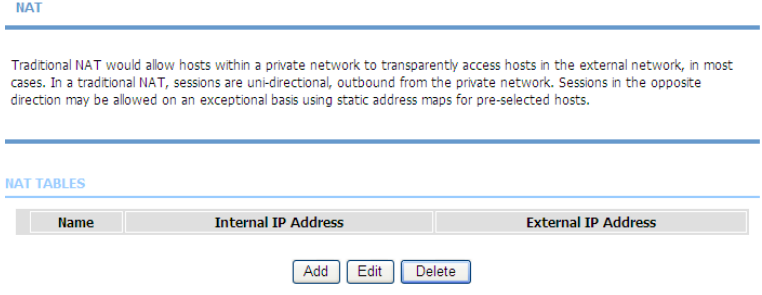
Choose **Advanced** > **Routing** and click **RIPng**. The page shown in the following figure appears. You can enable or disable dynamic routing of an IPv6 interface after establishing an IPv6 PVC connection.


RIPNG CONFIGURATION
To activate RIPng for the interface, place a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIPng based on the configuration.
RIPNG
Interface
VPI/VCI
Enabled
Apply
Cancel

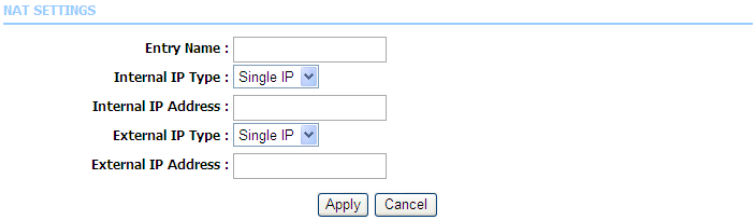
Click **Apply** to save the settings.

5.2.13 NAT

Choose **Advanced** > **NAT**. The page shown in the following figure appears. Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are unidirectional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts


NAT
Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts.
NAT TABLES
Name
Internal IP Address
External IP Address
Add
Edit
Delete

Click **Add** to set a NAT set in the following page. For IP type, you can choose single IP or IP range. Click **Apply** to save and enable the setting.

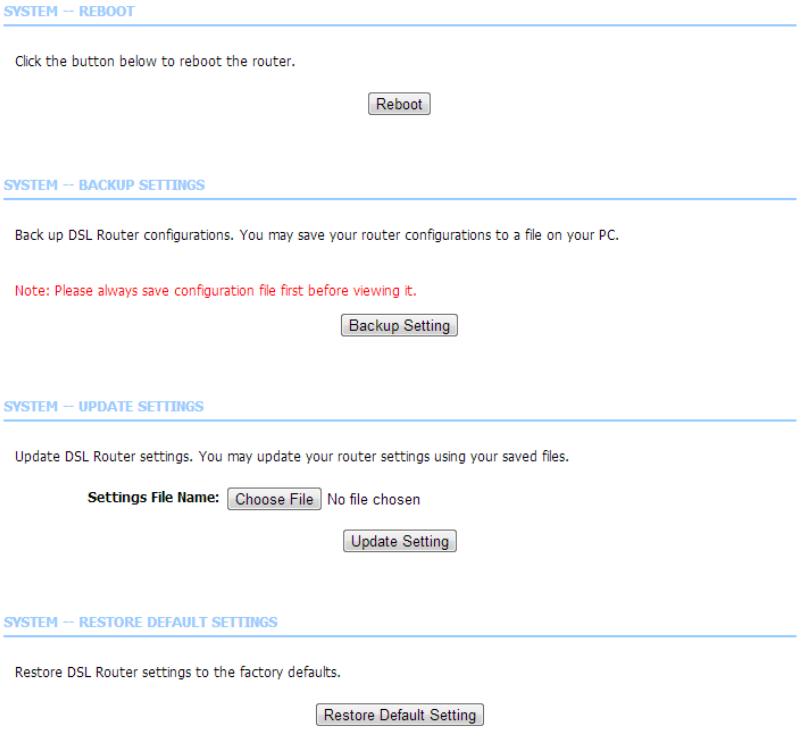


5.3 Management

In the main interface, click **Management** tab to enter the **Management** menu as shown in the following figure. The submenus are **System Management**, **Firmware Update**, **Access Controls**, **Diagnosis**, and **Log Configuration.**

5.3.1 System Management

Choose **Management** > **System Management**. The page shown in the following figure appears.


SYSTEM -- REBOOT
Click the button below to reboot the router.
Reboot
SYSTEM -- BACKUP SETTINGS
Back up DSL Router configurations. You may save your router configurations to a file on your PC.
Note: Please always save configuration file first before viewing it.
Backup Setting
SYSTEM -- UPDATE SETTINGS
Update DSL Router settings. You may update your router settings using your saved files.
Settings File Name:
Choose File
No file chosen
Update Setting
SYSTEM -- RESTORE DEFAULT SETTINGS
Restore DSL Router settings to the factory defaults.
Restore Default Setting

In this page, you can reboot device, back up the current settings to a file, update settings from the file saved previously and restore the factory defaults.

The buttons in this page are described as follows.

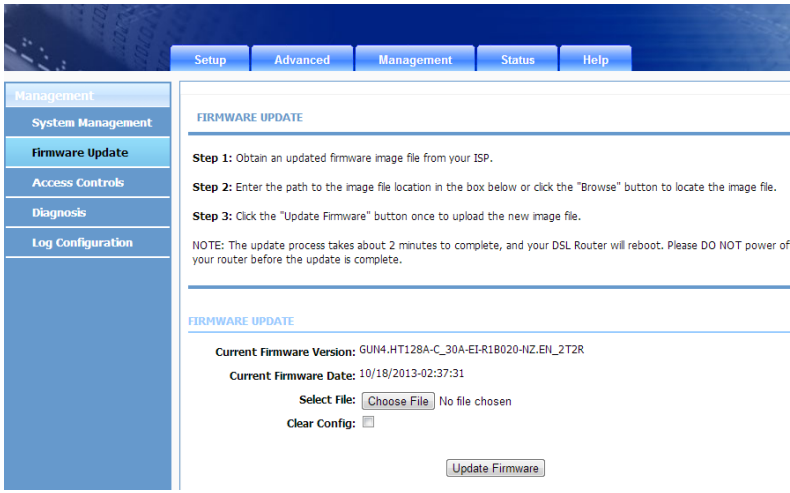
Field	Description
Reboot	Click this button to reboot the device.
Backup Setting	Click this button to save the settings to the local hard drive. Select a location on your computer to back up the file. You can name the configuration file.
Update setting	Click **Browse** to select the configuration file of device and then click **Update Settings** to begin updating the device configuration.
Restore Default Setting	Click this button to reset the device to default settings.

Note:

Do not turn off your device or press the Reset button while an operation in this page is in progress.

5.3.2 Firmware Update

Choose **Management** > **Firmware Update**. The page shown in the following figure appears. In this page, you can upgrade the firmware of the device.


Setup
Advanced
Management
Status
Help
Management
System Management
Firmware Update
Access Controls
Diagnosis
Log Configuration
FIRMWARE UPDATE
Step 1: Obtain an updated firmware image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Firmware" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.
FIRMWARE UPDATE
Current Firmware Version: GUN4.HT128A-C_30A-EI-R1B020-NZ.EN_2T2R
Current Firmware Date: 10/18/2013-02:37:31
Select File: Choose File No file chosen
Clear Config:
Update Firmware

To update the firmware, take the following steps.

Step 1 Click **Browse…**to locate the file.

Step 2 Select **Clear Config** to clear the current configuration and restore the default.

Step 3 Click **Update Firmware** to copy the file.

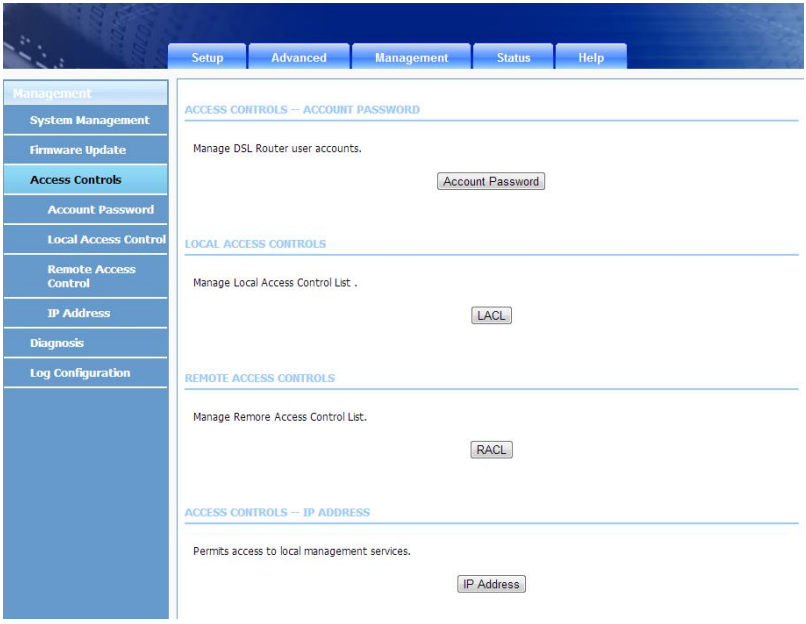
The device loads the file and reboots automatically.

Note:

Do not turn off your device or press the Reset button while an operation in this page is in progress.

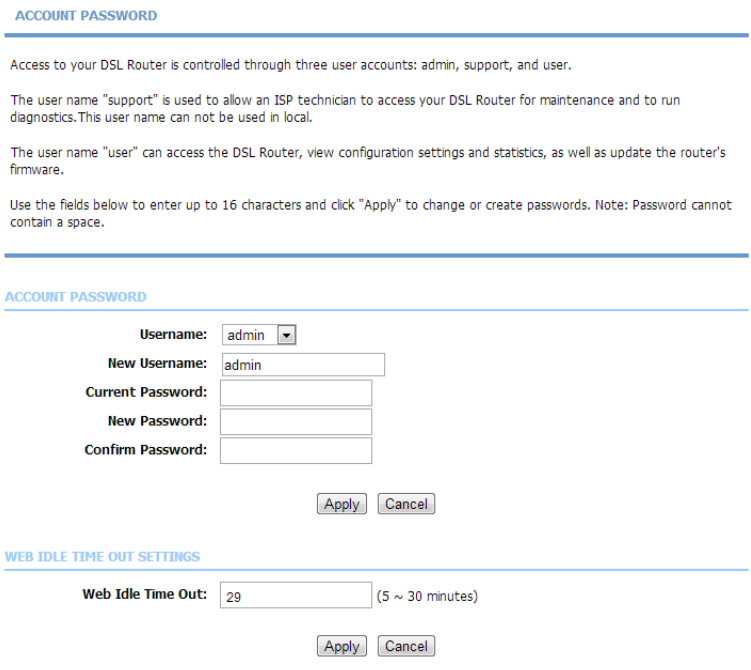
5.3.3 Access Controls

Choose **Management** > **Access Controls**. The **Access Controls** page shown in the following figure appears. The page contains **Account Password**, **Local Access Control, Remote Access Control** and **IP Address**.



5.3.3.1 Account Password

In the **Access Controls** page, click **Account Password**. The page shown in the following figure appears. In this page, you can change the password of the user and set time for automatic logout.


ACCOUNT PASSWORD
Access to your DSL Router is controlled through three user accounts: admin, support, and user.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.This user name can not be used in local.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as update the router's firmware.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
ACCOUNT PASSWORD
Username: admin
New Username: admin
Current Password:
New Password:
Confirm Password:
Apply Cancel
WEB IDLE TIME OUT SETTINGS
Web Idle Time Out: 29 (5 ~ 30 minutes)
Apply Cancel

You should change the default password to secure your network. Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you need to reset the device to the factory default settings and all configuration settings of the device are lost.

Select the **Username** from the drop-down list. You can select **admin**, **user** or **support**.

Enter the current and new passwords and confirm the new password to change the password. Click **Apply** to apply the settings.

Web Idle Time Out is the idle duration of user interfaces. After this duration, you need to login to the router again for operation.

5.3.3.2 Local Access Control

Under the **Access Controls** menu, click **Local Access Control**. The page shown in the following figure appears. This page allows you to enable or disable LAN management services. For example, if the Telnet service is enabled on port 23, the remote host can access the router by Telnet through port 23.

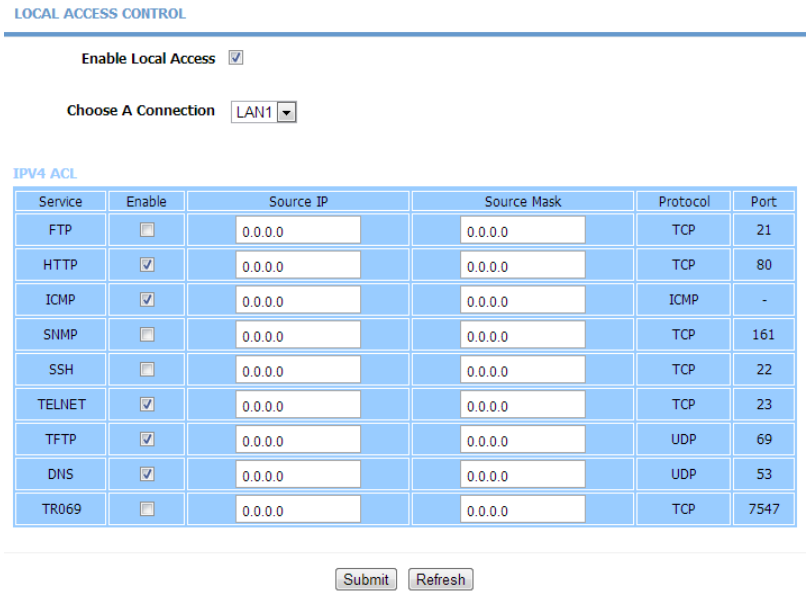


Figure 12

5.3.3.3 Remote Access Control

Under the **Access Controls** menu, click **Remote Access Control**. The page shown in the following figure appears. This page allows you to enable or disable WAN management services. You may refer to 5.3.3.2 Local Access Control.

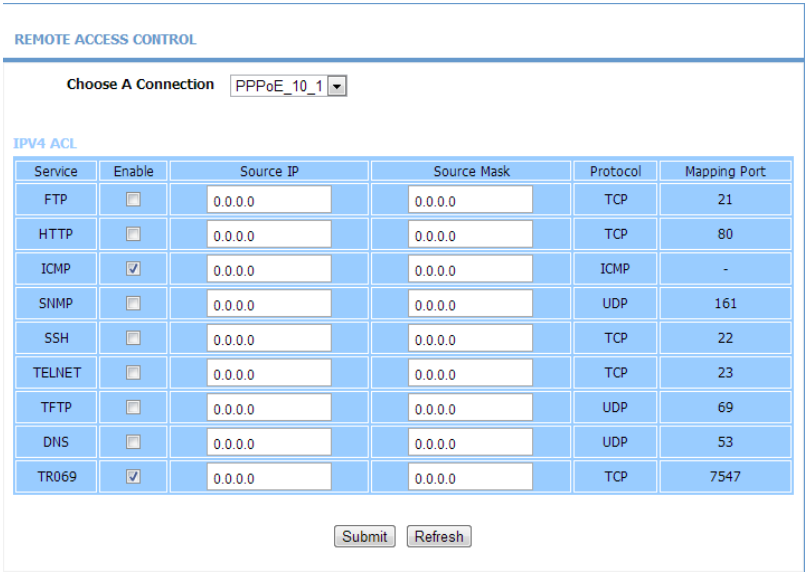
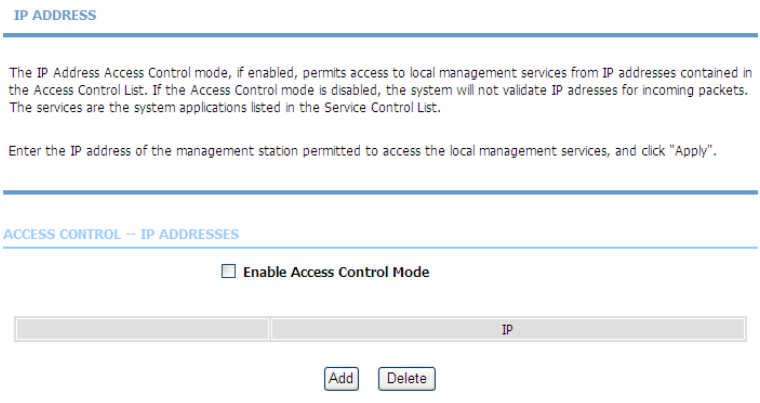


Figure 13

5.3.3.4 IP Address

In the **Access Controls** page, click **IP Address**. The page shown in the following figure appears.

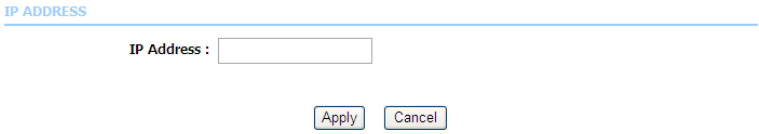

IP ADDRESS
The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP adresses for incoming packets. The services are the system applications listed in the Service Control List.
Enter the IP address of the management station permitted to access the local management services, and click "Apply".
ACCESS CONTROL -- IP ADDRESSES
Enable Access Control Mode
IP
Add
Delete

In this page, you can configure the IP address for access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device.

Note:

If you enable the ACL, ensure that IP address of the host is in the ACL list.

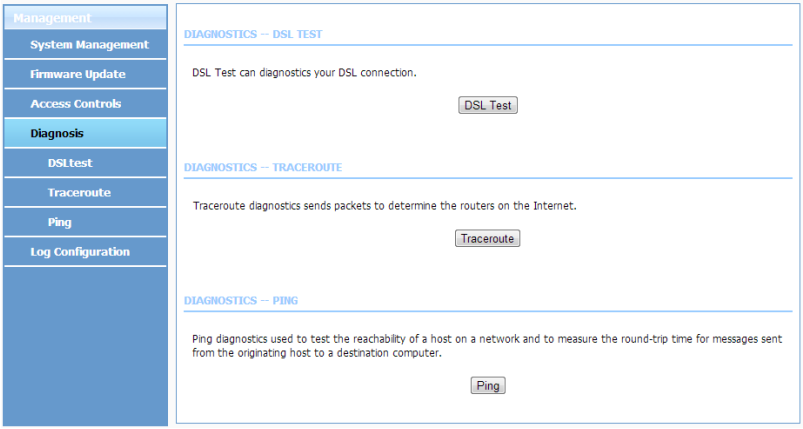
To add an IP address to the IP list, click **Add**. The page shown in the following figure appears.



Click **Apply** to apply the settings, and then choose **Enable Access Control Mode** to enable ACL.

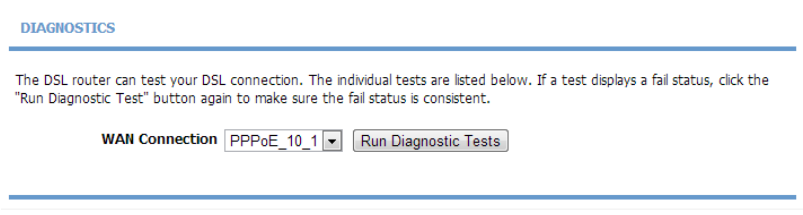
5.3.4 Diagnosis

Choose **Management** > **Diagnosis**. The **Diagnosis** page shown in the following figure appears. The page contains **DSL Test, Traceroute** and **Ping**.


Management
System Management
Firmware Update
Access Controls
Diagnosis
DSLtest
Traceroute
Ping
Log Configuration
DIAGNOSTICS -- DSL TEST
DSL Test can diagnostics your DSL connection.
DSL Test
DIAGNOSTICS -- TRACEROUTE
Traceroute diagnostics sends packets to determine the routers on the Internet.
Traceroute
DIAGNOSTICS -- PING
Ping diagnostics used to test the reachability of a host on a network and to measure the round-trip time for messages sent from the originating host to a destination computer.
Ping

5.3.4.1 DSL Test

In the **Diagnosis** page, click **DSL Test**. The page shown in the following figure appears. In this page, you can test your DSL connection.


DIAGNOSTICS
The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.
WAN Connection
PPPoE_10_1
Run Diagnostic Tests

Click **Run Diagnostic Tests**. After testing, the following figure appears.

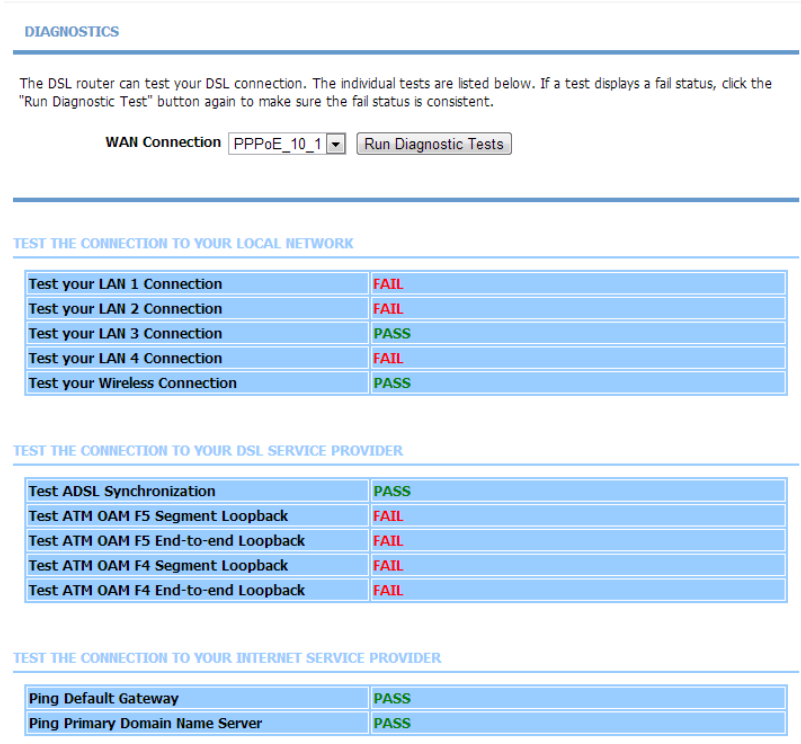
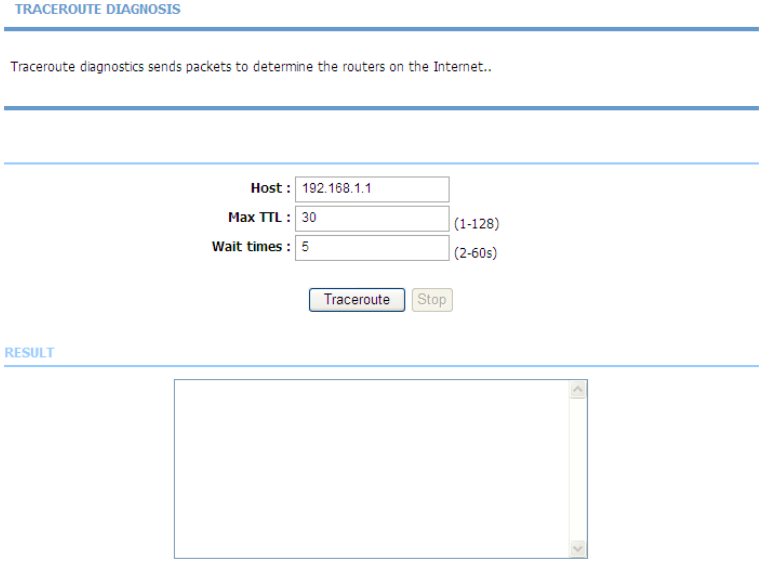

DIAGNOSTICS
The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.
WAN Connection
PPPoE_10_1
Run Diagnostic Tests
TEST THE CONNECTION TO YOUR LOCAL NETWORK
Test your LAN 1 Connection
FAIL
Test your LAN 2 Connection
FAIL
Test your LAN 3 Connection
PASS
Test your LAN 4 Connection
FAIL
Test your Wireless Connection
PASS
TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER
Test ADSL Synchronization
PASS
Test ATM OAM F5 Segment Loopback
FAIL
Test ATM OAM F5 End-to-end Loopback
FAIL
Test ATM OAM F4 Segment Loopback
FAIL
Test ATM OAM F4 End-to-end Loopback
FAIL
TEST THE CONNECTION TO YOUR INTERNET SERVICE PROVIDER
Ping Default Gateway
PASS
Ping Primary Domain Name Server
PASS

Figure 14

5.3.4.2 Traceroute

In the **Diagnosis** page, click **Traceroute**. The page shown in the following figure appears. In this page, you can determine the routers on the Internet by sending packets.



Click **Traceroute** to begin diagnosis. After finish, the page shown in the following figure appears.

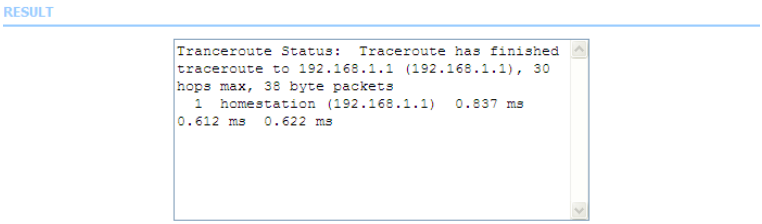
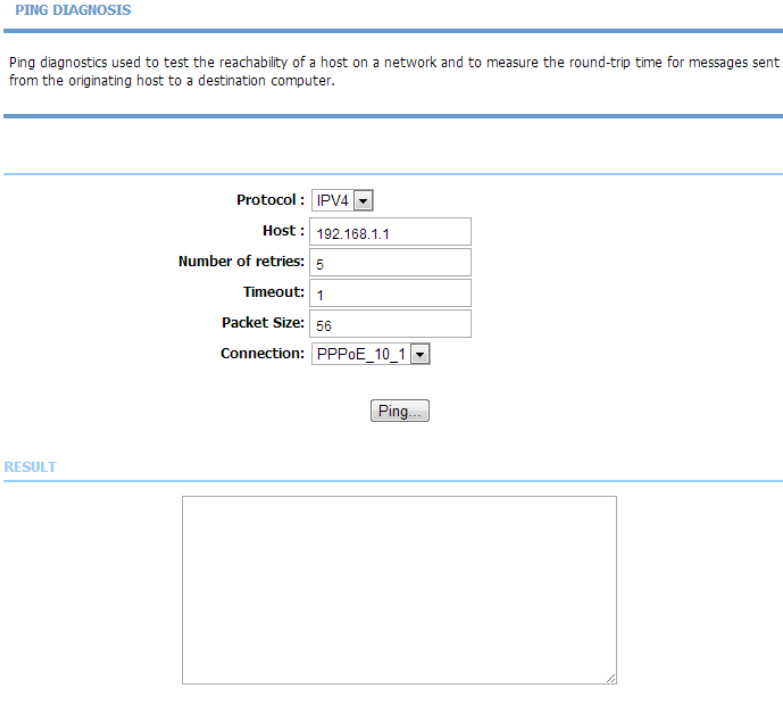

RESULT
Tranceroute Status: Traceroute has finished
traceroute to 192.168.1.1 (192.168.1.1), 30
hops max, 38 byte packets
1 homestation (192.168.1.1) 0.837 ms
0.612 ms 0.622 ms

Figure 15

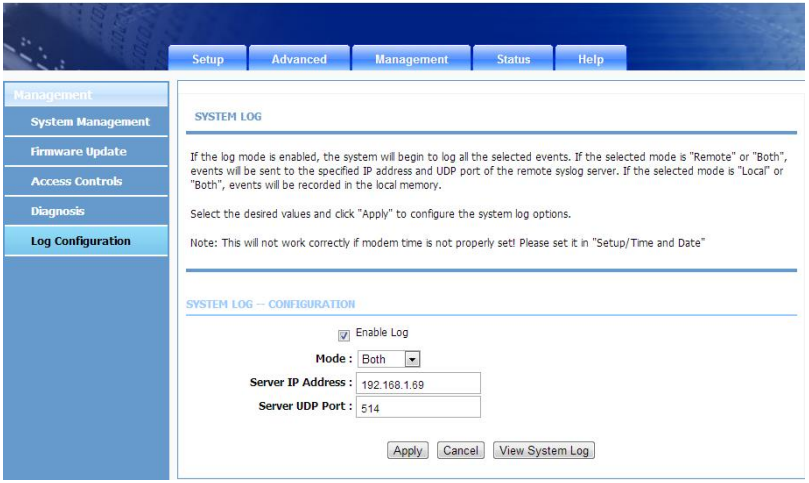
5.3.4.3 Ping

In the **Diagnosis** page, click **Ping**. The page shown in the following figure appears. In this page, you can determine the routers receive a response from a host IP/URL by sending packets


PING DIAGNOSIS
Ping diagnostics used to test the reachability of a host on a network and to measure the round-trip time for messages sent from the originating host to a destination computer.
Protocol : IPV4
Host : 192.168.1.1
Number of retries: 5
Timeout: 1
Packet Size: 56
Connection: PPPoE_10_1
Ping...
RESULT

5.3.5 Log Configuration

Choose **Management** > **Log Configuration**. The **System Log** page shown in the following figure appears.


Setup
Advanced
Management
Status
Help
Management
System Management
Firmware Update
Access Controls
Diagnosis
Log Configuration
SYSTEM LOG
If the log mode is enabled, the system will begin to log all the selected events. If the selected mode is "Remote" or "Both", events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is "Local" or "Both", events will be recorded in the local memory.
Select the desired values and click "Apply" to configure the system log options.
Note: This will not work correctly if modem time is not properly set! Please set it in "Setup/Time and Date"
SYSTEM LOG -- CONFIGURATION
Enable Log
Mode : Both
Server IP Address : 192.168.1.69
Server UDP Port : 514
Apply
Cancel
View System Log

This page displays event log data in the chronological manner. You can read the event log from the local host or send it to a system log server. In this page, you can enable or disable the system log function.

To log the events, take the following steps.

Step 1 Select **Enable Log** check box.

Step 2 Select the display mode from the **Mode** drop-down list.

Step 3 Enter the **Server IP Address** and **Server UDP Port** if the **Mode** is set to **Both** or **Remote**.

Step 4 Click **Apply** to apply the settings.

Step 5 Click **View System Log** to view the detail information of system log.

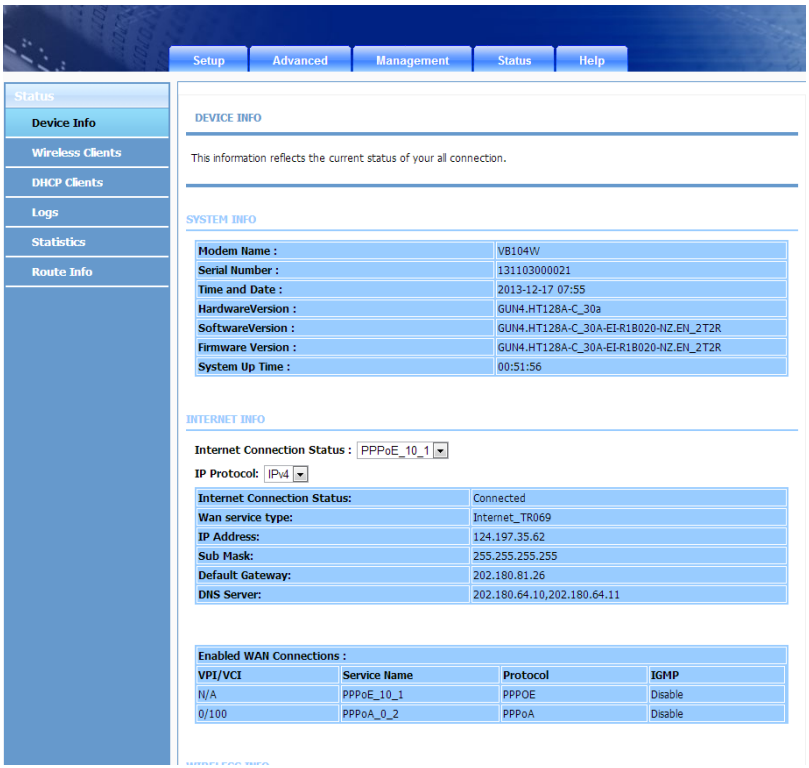
Figure 16

5.4 Status

In the main interface, click **Status** tab to enter the **Status** menu as shown in the following figure. The submenus are **Device Info**, **Wireless Clients**, **DHCP Clients**, **IPv6 Status**, **Logs**, **Statistics**, **Route Info** and **Logout**. You can view the system information and monitor performance.

5.4.1 Device Info

Choose **Status** > **Device Info**. The page shown in the following figure appears.



The page displays the summary of the device status. It includes the information of firmware version, upstream rate, downstream rate, uptime and Internet configuration (both wireless and Ethernet statuses).

5.4.2 Wireless Clients

Choose **Status** > **Wireless Clients**. The page shown in the following figure appears. The page displays authenticated wireless stations and their statuses.

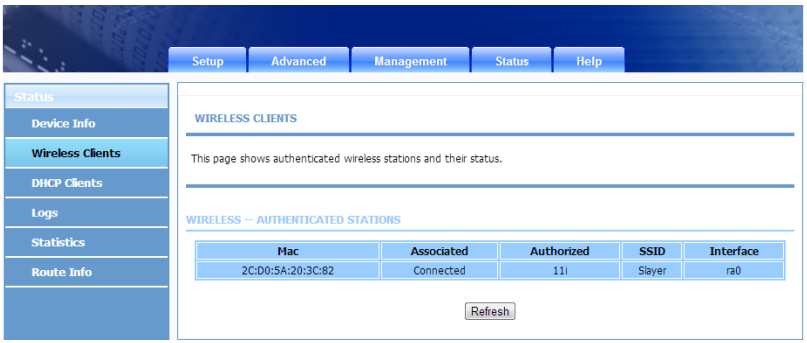
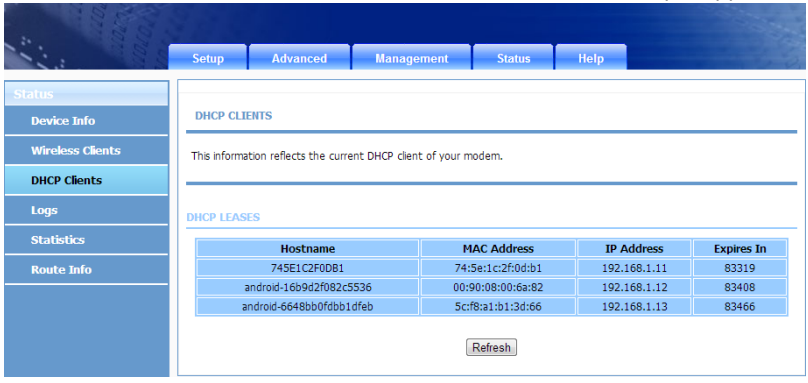


Figure 17

5.4.3 DHCP Clients

Choose **Status** > **DHCP Clients**. The page shown in the following figure appears. This page displays all client devices that obtain IP addresses from the device. You can view the host name, IP address, MAC address and time expired(s).



5.4.4 Logs

Choose **Status** > **Logs**. The page shown in the following figure appears. This page lists the system log. Click **Refresh** to refresh the system log shown in the table.

5.4.5 Statistics

Choose **Status** > **Statistics**. The page shown in the following figure appears. This page displays the statistics of the network and data transfer. This information helps technicians to identify if the device is functioning properly. The information does not affect the function of the device.

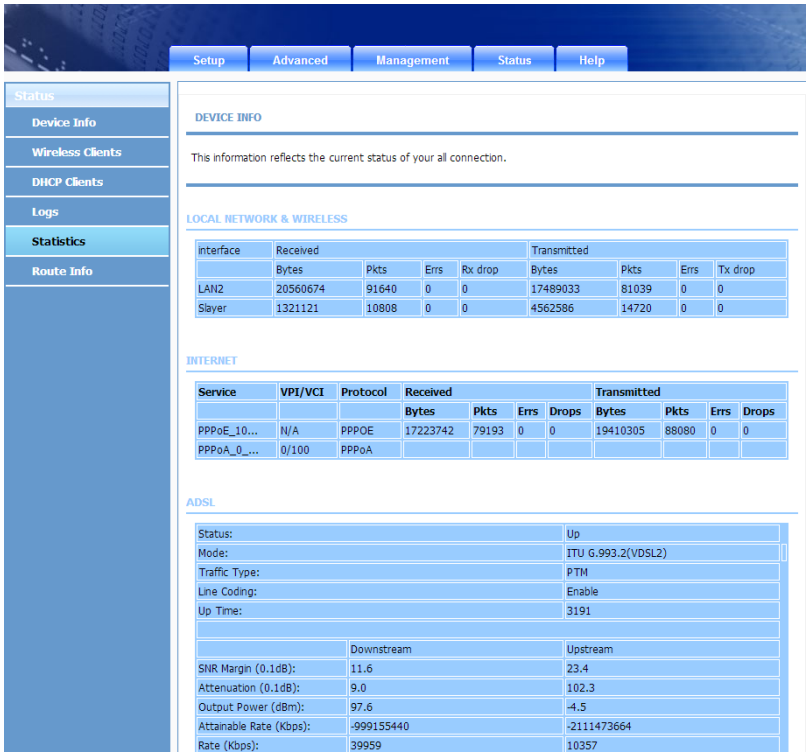

Setup
Advanced
Management
Status
Help
Status
Device Info
Wireless Clients
DHCP Clients
Logs
Statistics
Route Info
DEVICE INFO
This information reflects the current status of your all connection.
LOCAL NETWORK & WIRELESS
interface | Received | | | | Transmitted | | | |
| Bytes | Pkts | Errs | Rx drop | Bytes | Pkts | Errs | Tx drop
LAN2 | 20560674 | 91640 | 0 | 0 | 17489033 | 81039 | 0 | 0
Slayer | 1321121 | 10808 | 0 | 0 | 4562586 | 14720 | 0 | 0
INTERNET
Service | VPI/VCI | Protocol | Received | | | | Transmitted | | | |
| | | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Errs | Drops
PPPoE_10... | N/A | PPPOE | 17223742 | 79193 | 0 | 0 | 19410305 | 88080 | 0 | 0
PPPoA_0_... | 0/100 | PPPoA
ADSL
Status: Up
Mode: ITU G.993.2(VDSL2)
Traffic Type: PTM
Line Coding: Enable
Up Time: 3191
Downstream | Upstream
SNR Margin (0.1dB): 11.6 | 23.4
Attenuation (0.1dB): 9.0 | 102.3
Output Power (dBm): 97.6 | -4.5
Attainable Rate (Kbps): 999155440 | 2111473664
Rate (Kbps): 39959 | 10357

Figure 18

5.4.6 Route Info

Choose **Status** > **Route Info**. The page shown in the following figure appears. The table shows a list of destination routes commonly accessed by the network.

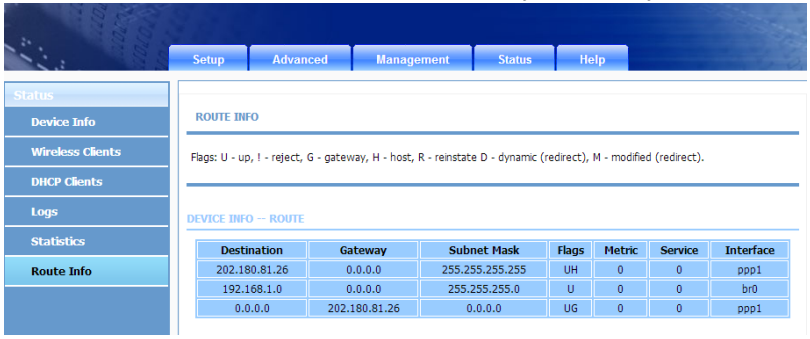
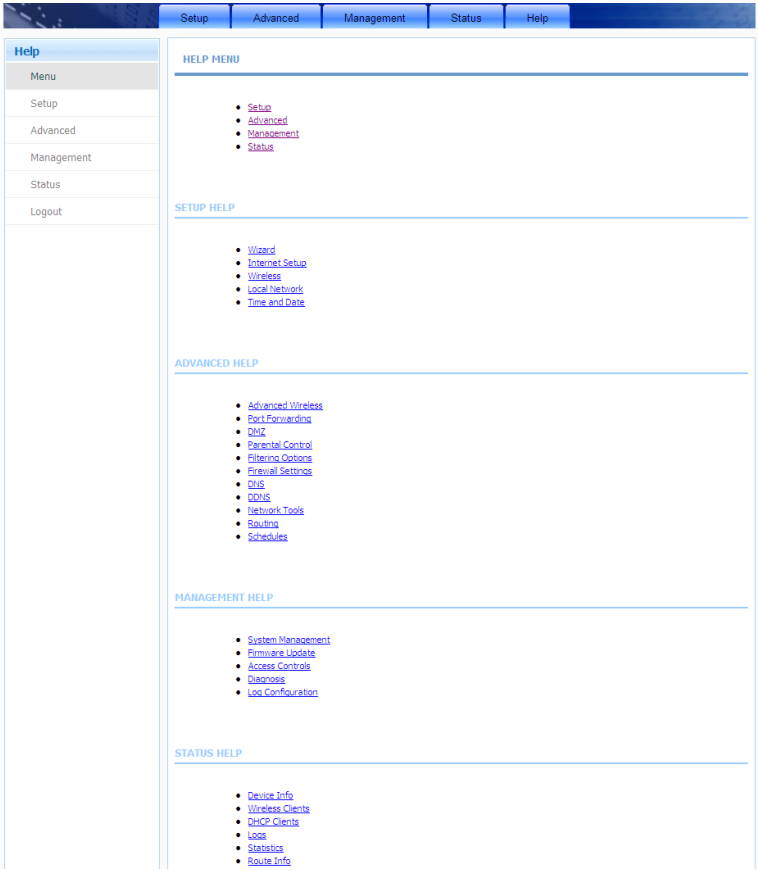


Figure 19

5.5 Help

In the main interface, click **Help** tab to enter the **Help** menu as shown in the following figure. This section provides detailed configuration information for the device. Click a wanted link to view corresponding information.



6 Trouble Shooting

Question	Answer
Why are all the indicators off?	● Check the connection between the power adapter and the power socket. ● Check whether the power switch is turned on.
Why the **LAN** indicator is off?	Check the following: ● The connection between the device and your PC, hub or switch ● The running status of the computer, hub, or switch
Why is the **DSL** indicator not on?	Check the connection between the **DSL** port of the device and the wall jack.
Why Internet access fails while the ADSL indicator is on?	Check whether the VPI, VCI, user name and password are correctly entered.
Why I fail to access the web configuration page of the DSL router?	Choose **Start** > **Run** from the desktop, and ping ***192.168.1.1*** (IP address of the DSL router). If the DSL router is not reachable, check the type of the network cable, the connection between the DSL router and the PC, and the TCP/IP configuration of the PC.
How to load the default settings after incorrect configuration?	To restore the factory default settings, turn on the device, and press the reset button for about 3 seconds, and then release it. The default IP address and the subnet mask of the DSL router are **192.168.1.1** and **255.255.255.0**, respectively. ● Administrator username/password: **1234**/**1234** (subject to different models). ● Common username/password: **user**/**user**. ● ISP technician username/password: **support**/**support**.